大成 DENTONS KENSINGTON SWAN

Independent review of access to and use of client information at ACC

May 2022
Reviewer: Linda Clark

Table of contents

Part I
Introduction

1 Introduction

1 The Accident Compensation Commission **(ACC)** was established in 1974 to administer a unique social contract under which any citizen, resident or temporary visitor who suffers personal injury in New Zealand is provided with compensation, recovery and rehabilitation services but does not have the right to sue for their injury.

2 Under this social contract, ACC holds personal information on every person who ever suffered an injury in a road smash, a workplace accident, on the sports field, in the gym, at home in the garage or the kitchen and who then lodged a claim with ACC. This information sits at the epicentre of ACC's core business, which is assisting the injured to recover and rehabilitate. Without information about each client, their health status, their treatment options, and their recovery progress ACC could not meet its responsibilities under the Accident Compensation Act 2001 **(AC Act)**. Nor would it have valuable data with which to analyse injury trends and recovery outcomes.

3 While the information ACC collects, stores, accesses, uses, discloses and ultimately destroys includes details about each individual's health and well-being, it can also include information about such things as family circumstances, lifestyle choices, mental health, the death of a child and, where applicable, histories of abuse. Information of this kind is highly personal, usually confidential and sensitive. All of it is personal information as defined by the Privacy Act 2020 (**Privacy Act**).[1]

4 Information of this character is protected by statute. But even if that was not the case, the nature of the relationship between individuals and ACC means clients are entitled to expect that the information they share with ACC will be treated as both personal and precious. We refer to clients' personal information in this Review as a taonga, because it is information that each client concerned holds closely and that needs to be handled carefully and respectfully. Every ACC worker who, for whatever reason, has access to this personal information must understand this, respect it and take every step to ensure this trust is neither taken lightly nor abused. One of the tasks for this Review was to test whether such a mature understanding and respect for privacy is embedded in the organisation.

5 This Review was commissioned in November 2021 by the Board of ACC following media reports of two separate incidents. We refer to these as the Access Incident and the Snapchat Incident. The first involved a client distressed to discover that his file, including his 'sensitive claim', had been accessed by more than 90 ACC personnel. The second incident involved a group of call centre workers initiating a Snapchat group on which two workers shared screenshots of client information while other workers posted supposedly humorous comments. One of the screenshots contained information which would identify a client.

6 In the wake of these incidents, the Board asked for a review into the access and use of client information within ACC, including a review of systems and policies in relation to access and use of client information, the oversight, monitoring and auditing of access and use and on-going training related to access and use of client information. The Board also asked the Review to address issues arising from the incidents. (The Terms of Reference for this Review are set out in **Schedule 1**).

7 From December 2021 until February 2022 (allowing for the summer break) we interviewed ACC staff from different parts of the business, different roles, different offices and with different lengths of service at ACC. All interviewees were encouraged to speak candidly, and they did. We reviewed all relevant ACC policies, training material and manuals and, where required, we made requests to ACC for additional information — all of which were answered. In February 2022, ACC provided a summary of an internal review of 'management of customer information' which identified changes ACC has

[1] Privacy Act 2020, s 7(1).

either made or is investigating following the Access Incident. Some of these initiatives touch on the issues discussed in this Review (we refer to these in this Review as the **Improvement Initiatives).**

8 At the latter part of the Review we also sought to 'sense check' certain information with privacy specialists at two Government agencies, both of which manage large quantities of personal information. After a draft report had been prepared (but before the report was finalised) we consulted with the Acting Privacy Commissioner, Liz McPherson. and with Treasury, ACC's external monitor. Material from all of these sources has been used to inform this report.

9 Throughout this report verbatim quotes are used. These quotes are from ACC staff who agreed to be interviewed for this Review. All interviews were conducted on the basis of anonymity and so the identity and position of each staff member has been withheld.

10 During the life of this review a number of ACC clients and other members of the public also contacted me directly, seeking to have complaints or concerns investigated as part of the Review. Such investigations into specific complaints are beyond the scope of the Terms of Reference of this Review. In each case, individuals were directed to ACC's own complaints service or the Office of the Ombudsman, as appropriate. To the extent that members of the public have concerns about their own privacy in their dealings with ACC, I am confident the recommendations contained in this Review, if implemented, will provide greater protection and more comfort.

11 Lastly, I wish to thank all those ACC staff who offered their experience, insights and observations to this Review. While this Review contains criticism of ACC's overall privacy management, it is not intended to be read as a condemnation of the organisation as a whole, or any individuals in particular.

Linda Clark
Reviewer

Part
Summary of findings and recommendations

2 Summary of findings and recommendations

Summary of findings

12 From the first interview conducted for this Review it was apparent that ACC staff believe they work in an organisation with a strong privacy culture. In large part this self-belief is the product of a decade of initiatives following an earlier high profile privacy breach and the comprehensive 2012 review by KPMG which followed it **(2012 Independent Review).**[2] All interviewees, without exception, expressed disappointment and censure for the acts of the individuals involved in the Snapchat Incident. One interviewee became tearful describing the harmful effect such a privacy breach would have on clients' trust in ACC.

13 This Review intends no criticism of any staff member nor of the organisation as a whole. ACC plays a vital role in New Zealand, managing millions of injury claims. Every working day ACC receives (on average) 9,088 new claims,[33] and it processes more than two million claims per year. It had not experienced a major privacy breach since 2011 and, without minimising what occurred then, that breach was due to human error. It is also evident that since 2012 the organisation has taken steps to improve its privacy mindset, and in respect of certain kinds of privacy breaches those steps have been successful. Since the two incidents which prompted this Review, ACC has also embarked on a programme to improve its management of personal information, although this programme remains a work in progress, with some aspects merely at the very preliminary stage.

14 Nonetheless, this Review concludes that ACC's overall privacy culture is not strong and that there is work to be done before all staff fully understand what is required to be protectors of client information. We identified gaps, both in the systems ACC depends on and in the organisation's overall culture.

15 In short, we found that:

a ACC staff have an understanding of personal information and their obligations to protect it which has been largely informed by the privacy breach of 2011 and the organisation's extensive efforts to avoid any such similar breach happening again.

b The fact the 2011 breach involved the inadvertent sending of client information to an unauthorised person has significantly influenced what ACC staff understand a breach of privacy to be. As a result, ACC has developed an asymmetrical privacy culture in which staff have a good understanding of the implications of sending client information to unauthorised third parties, but an incomplete understanding of privacy overall.

c ACC's policy focus is narrowly configured at consideration of privacy breaches to external parties to the detriment of other kinds of breaches, including those between staff. As a consequence, while significant effort has gone into minimising the risk of external release breaches, insufficient effort has gone into identifying or reducing other potential misuses of client information.

d ACC's privacy management is reactive, rather than proactive. It is focused on responding to breaches rather than actively managing personal information in line with the Information Privacy Principles **(IPPs)** as set out by the Privacy Act.[44]

e The organisation has undergone a sustained period of change to improve efficiency and responsiveness, particularly in the context of ACC's implementation of the Next Generation Case Management model (**Next Generation**). Clients have benefited from this, even though one effect of the changes has meant more eyes will access the personal

[2] The 2012 Independent Review by KPMG followed the inadvertent disclosure of the details of 6,748 clients, which occurred on 5 August 2011

[3] Average per day based on 250 working days and the total number of claims received in the 2020/21 financial year (2,272,085).

[4] Privacy Act 2020, s 22.

information of some clients. But there is a balance to be struck between ensuring operational efficiency and protecting individuals' privacy. It is not clear to us that ACC has struck this balance fairly.

f For operational reasons, ACC employs a high trust approach to access to client information, which staff almost universally support and defend. Staff in client facing roles have open gate access to the majority of client information.

g ACC does not have adequate monitoring and auditing processes to provide oversight of staff access to and use of client information. This means, for example, that it is not possible to say with confidence that staff do not browse client information, since no system exists to test this. Instead, managers rely on a certain belief that staff are too busy to browse.

h Staff induction and privacy training lacks a comprehensive focus on what personal information is, the full range of potential breaches to avoid, and all of the obligations on staff to protect a client's privacy.

i ACC's internal-facing privacy policy is out of date; it refers to statutes that have been replaced and identifies authority for implementation of policy to a position within ACC that has been disestablished.

j Implementation and oversight of privacy-related policy within ACC is currently overseen in practice across different parts of the organisation.

16 In an organisation such as ACC where personal information is central to the organisation's core business, privacy protection needs to be embedded at every level and in every interaction. This requires strong leadership, thorough policies, reliable and rigorous monitoring and auditing, and continuous staff training. It cannot be achieved by the privacy team working alone, particularly when (as happens) privacy related issues are managed in silos across the organisation and therefore the dedicated privacy team does not always have visibility of issues as they arise. All staff need to have a clear road-map setting out what is expected of them, how they must comply with those expectations and who to turn to if they don't understand their obligations or they see conduct that breaches those obligations. This requires a holistic, values-based approach through which protection of client information is well understood and positively modelled by team leaders, the senior leadership team, and the Board.

17 The cover this Review shows two hands, gently cupped as if holding a precious object. ACC holds clients' personal information in its hands every day. New Zealanders trust it to hold their personal information safely and lawfully. As we have seen, they are distressed when they discover that this information has not been handled in such a careful way.

18 The 2012 Independent Review conducted made 44 recommendations. Among them were recommendations that ACC:

a strengthen its organisational culture to emphasise respect for individuals and personal information that is collected, stored and used by ACC; and

b strengthen privacy accountability across the whole organisation by ensuring that staff roles and responsibilities for privacy are clearly identified.

19 This Review endorses these recommendations. ACC made demonstrably good progress following the 2012 Independent Review. As a consequence, the Board can have confidence that staff follow the procedures now in place to avoid client information being sent to an unauthorised third party. Across the organisation this type of breach is well understood and there are safeguards to ensure staff are constantly alert to the risk. But this is just one kind of potential privacy breach and understanding and safeguarding against other potential breaches remains a work in progress.

20 The latest incidents provide ACC with an opportunity to reset its privacy protections and to initiate a second wave of improvements. This work should enable ACC to both strengthen its organisational culture and its privacy accountability and in doing so retain public trust and confidence.

Summary of recommendations

21 Generally, this Review recommends that ACC agree a process with the Office of the Privacy Commissioner **(OPC)** for regularly updating the OPC on ACC's progress in implementing the recommendations made by this Review. We recommend that, at least for the first year, ACC provide updates on progress to the OPC every two months.

22 This Review makes recommendations in respect of ACC's policies and procedures (see Part 5), systems and process (see Part 7) and privacy culture (see Part 8). Those recommendations are summarised in the table below.

PART 5 (POLICIES AND PROCEDURES	
R5.1	Consider a reformulation of the five lines of assurance model for the Privacy Policy, with a view to improving accountability for privacy at an executive level and above.
R5.2	Allocate responsibility for the application, enforcement, and management of the Privacy Policy to a member of the executive team, consider how best to ensure that appropriate mandates and structures are in place to clearly drive opportunities for updates to the Privacy Policy, and put processes in place to ensure those changes can occur across all parts of ACC's business.
R5.3	Review and update the Privacy Policy to reflect and incorporate: • changes to legislation and best practice; • changes to ACC's organisational structure; • the client information roadmap, prepared in accordance with **R7.1;** • clear expectations about managing client information, including providing practical guidance on what staff should and should not do to ensure client information is protected; and • more regular reviews (for instance, on an annual basis) and accountability mechanisms to better ensure the document remains up to date (in accordance with the processes put in place in response to **R5.2).**
R5.4	Review and update the Code of Conduct to reflect and incorporate: • changes to legislation and best practice; • clear expectations about managing client information, including inappropriate behaviours such as browsing of client files; and • more regular reviews (for instance, on an annual basis) to better ensure the document remains up to date.
R5.5	Review and amend the Integrity Policy with a view to ensuring that: • it is clear to ACC staff that misuse of client information is an integrity incident; • misuse of client information is defined broadly; and • staff understand activities such as browsing of client files would be considered an integrity incident for the purposes of the policy.
R5.6	Consider how the Integrity Policy can be strengthened so that it is the 'backbone' of ACC's callout culture and so that ACC can be sure that: • staff are made aware of the policy and the processes contemplated by the policy (including so that staff are generally aware of what they should do if they come across an integrity incident); • all integrity incidents are reported under the policy and staff are cognisant of the importance of raising incidents internally to give ACC the ability to put matters right; and • staff are empowered to use the policy and given confidence that their reports will be taken seriously.

R5.7	Assess the impact on staff of working from home, particularly for frontline staff, and consider what additional measures can be put in place to ensure staff have a safe and secure way to stay connected, including the opportunity to debrief safely.
R5.8	Introduce a working from home policy that includes (at a minimum): • clear expectations as to how personal information should be protected while working from home, for example, working from a separate room from other members of the household where possible, limiting the use of paper documents used at home, not working near windows or high traffic areas, ensuring all calls are taken in private and so on; • a broad application to all ACC staff who work from home or at another location, whether via a formal arrangement, in an emergency or on an ad hoc basis; • a clear requirement that only ACC approved devices should be used when working from home; and • guidance for staff on what communication channels should be used when working from home when discussing client information.
R5.9	Implement a social media policy that includes at least the following: • a clear and comprehensive statement that client information should never be shared on social media or on a personal device, even if anonymised and even if the sharing is only with other ACC staff members; • an acknowledgement that social media channels can be legitimately used by teams and groups of staff members, while also putting in place clear guidelines setting out what is and isn't acceptable use of these channels; • guidance to ensure that staff are aware that any work related information shared on personal devices or social media is discoverable under the OIA and Privacy Act; and • a preference that staff who are provided work devices use these for work discussion wherever possible (for example, if there is a need to text one another they do so on their work device rather than their personal device), and guidance for staff that do not have work devices that these should not be used for work related discussions unless absolutely necessary.
PART 7 (SYSTEMS)	
R7.1	Undertake a comprehensive client information mapping exercise, for which an executive team member is responsible, for the purposes of creating a clear, complete, and accurate overview of how client information is managed within ACC, from the point of ACC's collection and receipt of that information through to its destruction. That map should remain 'live' and subject to regular review, particularly where and when new systems are introduced.
R7.2	With reference to the client information map prepared in accordance with **R7.1,** ensure that disclosures made to clients about how their information is managed are accurate, such that ACC's approach to client information (including the circumstances in which a client's file may be viewed by ACC personnel) is clearly understood by clients. Consider introducing a 'customer facing' version of that road map.
R7.3	Undertake a comprehensive review of the role mapping dictionary that currently exists. An executive team member should lead this, for the purposes of establishing clear guidelines for when any one role will be granted access to EOS, the conditions of that access, and the circumstances in which that access should be reviewed or removed. Such guidelines should be well managed, documented, and understood across all levels of the organisation.

R7.4	Develop and implement a comprehensive and regular permissions review processes, for which an executive team member is responsible, so that ACC can satisfy itself that only those who need to have access to client information actually have access. We would anticipate this process to involve a mixture of automated processes which are supported by ACC's current approach to managers confirming their team member's access, as well as regular accountability checks to ensure those processes are working as intended.
R7.5	Investigate the ways graduated access can be implemented in respect of 'general' claims in a way that does not materially jeopardise ACC's ability to efficiently handle claims. That process should involve at least the following steps: • Following the role-mapping exercise recommended at **R7.3** above, ACC should identify the which roles require access to EOS and, with respect to each of those roles, the extent of access required for that role (having regard to the role description and responsibilities). Our suggestion is that ACC start from the assumption that full open gate access is not necessary for the majority of roles. • Investigate the introduction of a 'confirm access required' function to appear on screen before any access is permitted to certain types of tabs and/or files. If this function can be added, identify and publish the types of tabs and/or files to be gated in this way. We recommend all medical notes, including notes provided by psychologists, psychiatrists and counsellors be included. • ACC should then analyse the actual inefficiencies that are likely to be introduced if graduated access is rolled out (rather than just perceived inefficiencies). • Once those inefficiencies have been identified, ACC should consider the materiality of those efficiencies, in the broader context of ACC's statutory functions and its obligations under the Privacy Act.
R7.6	Introduce enhanced and regular monitoring and auditing procedures, including 'spot checks', to test access permissions, and to confirm that staff access to and use of client information complies with ACC's privacy obligations (as well as all relevant ACC policies).
R7.7	Appoint a member of the executive team to be responsible for the development and implementation of the regular, randomised, and proactive checks of access described in **R7.6.**
R7.8	Implement a clear policy, for which a member of the executive team is responsible, which establishes the consequences for workers if the above checks reveal inappropriate access to client information.
R7.9	Ensure that the policies and procedures put in place in accordance with **R7.6** and **R7.8** are well understood across ACC (which may include putting in place appropriate mandates and structures to support the implementation of the policy across the organisation).
R7.10	Prioritise the Improvement Initiative to enhance ACC's digital footprint capability with a view to actually implementing (and then using, in accordance with a well-documented and publicised policy) granular auditing tools as soon as practicable.

PART 8 (CULTURE)	
R8.1	Conduct a comprehensive review of the various tools, systems, documents and guidance ACC currently uses to shape its privacy culture and consider how these can be modified to ensure that all staff are taught that key privacy values, such as the fact that privacy is important and that it should be protected at all costs. This review should include, at the least, the following: • Consideration as to whether the current tools such as privacy newsletters or the use of the privacy team to answer questions, are effective at delivering broader cultural messages. Assess what other options, such as a values statement or other guiding principle, may assist to develop this privacy culture. • The introduction of measures and targets to gauge the strength of its privacy culture and performance that go beyond breach reporting. For example, ACC could implement measures and/or targets in respect of the completion rates of privacy training, number of visits to the privacy intranet page, and staff surveys on awareness and understanding of privacy values. ACC could also measure and assess the questions the privacy team receive from staff to identify gaps in understanding and put in place refresher training or further guidance to plug these gaps.
R8.2	Implement changes to the organisational structure, capability, and mandate of the privacy team (including the Privacy Officer role) to ensure: • that the privacy team has sufficient influence to bring about change where required. This should include a consideration of whether any changes are required to role descriptions, resourcing or the privacy team's day-to-day tasks to allow them to spend more time building (and measuring) ACC's privacy culture and working to build a set of privacy values; • that a member of the executive has overall accountability and responsibility for privacy; • that measures are put in place to support enterprise wide execution and support of changes recommended by the privacy team; and • that the executive leadership team has sufficient oversight of privacy matters that goes beyond reporting on breaches.
R8.3	Consider how to ensure that PETA and PIA assessments are not a 'box ticking' exercise. As part of this ACC should consider how to ensure that privacy assessments are done *before* a new system or model is put into motion, rather than after.
R8.4	Asses what changes are required to ensure that PETAs and PIAs are afforded sufficient weight within the organisation. This should include: • requiring PETAs and PIAs to be signed out by the Head of Privacy to ensure that the assessments are given a greater degree of importance throughout the organisation; and • requiring the Head of Privacy to provide quarterly reports to a member of the executive about the number of assessments and the recommendations made.

R8.5	Review the thresholds for when privacy assessments are required. This should include: • ensuring that PIAs and PETAs are completed that when there are major changes to systems or work practices (such as a move to working from home) rather than only when new systems are introduced; and • considering whether a PETA/PIA (or full PETA/PIA) is required for every systems change.
R8.6	Consider implementing an organisation-wide education programme on the many different ways privacy can be breached, and take steps to ensure that this knowledge and understanding becomes embedded in the organisation's culture.
R8.7	Undertake a comprehensive review of ACC's privacy training, including to address the gaps identified in ACC's induction and ongoing training. Such review should consider at least the following: • Ensure privacy training modules and associated material (for example, the intranet page) adequately teach staff key values, including the importance of privacy and protecting personal information. • Ensure privacy training covers all aspects of the IPPs — collection, retention, use, sharing, and disposal of personal information. • Put in place annual refresher training (we understand that ACC, as part of its Improvement Initiatives, is currently considering a new approach to re-engagement activities, such as Privacy Week, but we would recommend that it actively consider annual refresher training in addition to re-engagement activities). • Consider what additional training may be necessary for different types of staff. For example, younger staff members or employees that are new to employment or the public service may need more targeted or detailed training. • Ensure all staff are required to actually complete privacy training and other modules within one month of commencing their employment at ACC. • Remove the ability for staff to 'skip' through training modules so that all trainees are required to answer the questions posed by the modules.
R8.8	Complete a detailed review of its callout culture (in addition to the review of its Integrity Policy recommended at **R5.5** and **R5.6)** to ensure that there is a robust system in place to enable staff to raise concerns anonymously and without fear of retribution.
R8.9	To better ensure that all breaches and near misses are reported, ACC's review of its callout culture should consider what changes can be made to the privacy breach reporting tool to ensure staff are aware of the different types of breaches that can and should be reported.
R8.10	Consider how to shift the focus from claims to clients across corporate documents, training and performance measures, to ensure that the client or customer is always front and centre (and recognising that language is an important tool to embed values).
R8.11	Give consideration to how the word 'sensitive' is currently used to denote personal information that requires additional legal protection. In staff induction and training, consider how to provide education on the fact that all personal information, not just 'sensitive' information has and requires legal protection under the Privacy Act and other legislation.

Part 3 - Overview of Snapchat and Access Incidents

3 Overview of Snapchat and Access Incidents

23 This Review is required to address the 'issues arising from the recent alleged inappropriate access and use of client information among ACC staff and resulting privacy breaches'. Those incidents referred to are:

a reportedly high volumes of ACC staff accessing a 'closed' sensitive claim **(Access Incident);** and

b the creation of a Snapchat group named 'ACC Whores', in which ACC workers shared and commented on client information **(Snapchat Incident).**

24 In accordance with the Terms of Reference:

a this Review sought to understand the facts relating to each incident for the purposes of identifying what issues arose from those incidents; but

b the Review did not set out to independently investigate the incidents or make findings of fault in respect of any individual at ACC. Those matters are outside the scope of this Review.

25 We set out the facts of each incident below.

The Access Incident

26 On 12 October 2021, Radio New Zealand **(RNZ)** published a report that an ACC client was 'horrified' to discover that 92 ACC staff had accessed his sensitive claim file.[5] The report was the result of RNZ's investigations of ACC between 1 July 2021 and 11 October 2021. For ease of reference, this section refers to the client's complaints to RNZ as the 'Access Incident'. We refer to this client as 'M'.

27 According to the RNZ report:

a M filed a sensitive claim with ACC in 2016. Sensitive claims are for mental or physical injuries caused by a specified criminal act.[6] It is standard practice for staff access to sensitive claims to be more limited than access to general claims due to the circumstances which typically led to the injuries being sustained and the injuries themselves.

b M then undertook 10 'pre-cover sessions' and a formal sensitive claim assessment with a therapist.

c In February 2017, M 'closed' the sensitive claim file, but continued to receive cover for sessions with a psychiatrist in respect of a separate physical injury claim.

d In June 2020, M met with ACC staff for the purposes of discussing cover for a mobility aid to assist with recovery from the physical injury.

e Following that meeting, ACC emailed M to report that an ACC-appointed physiotherapist advisor was reviewing the request for assistance and had suggested that the basis of the previous sensitive claim may also be relevant to the current injury. That email recorded that the ACC physiotherapist had recommended M be reassessed by a neuropsychiatrist.

f The client's advocate told RNZ:

> Basically, [the physiotherapist] said, I can see that he has a sensitive claim, but I'm unaware of the details of the claim.

[5] The report remains published an the RNZ website under the heading *'Man horrified 92 ACC staff accessed his sensitive claims file'*

[6] Accident Compensation Act 2001, Schedule 3 sets out a list of criminal acts which cause mental injuries that would be considered a sensitive claim under the Act

> However, [she said] this may influence the condition and it needs to be assessed. So we want permission from him to open this up and give it to someone to be assessed. And until that's done, [we] don't provide any other treatment or rehabilitation.

g M and the his psychiatrist continued to correspond with ACC, rejecting any link between the client's physical injury and the earlier sensitive claim.

h In December 2020, M and ACC staff met via Zoom. Following that meeting, M requested a copy of the digital 'footprint' for his file. The media report noted that the footprint showed:

i 92 different ACC staff from 'around the country' had accessed M's sensitive claim file;

ii M's file had been accessed 356 times since 2017 when he closed the claim;

iii the ACC physiotherapist advisor who had suggested the sensitive claim be reassessed, had accessed M's file four times (twice before she recommended M give his permission to allow the claim to be read by new assessors, and twice afterwards);

iv M's file had been accessed by reportedly 'dozens' of different ACC clinical advisors, cover assessors, a former case manager, and administration staff in Auckland, Wellington, Hamilton, Timaru, and Dunedin.

i M requested that ACC immediately prevent staff from accessing his sensitive claim file.

j M's advocate made further enquiries with ACC's Privacy Officer and filed requests for information under the Official Information Act 1982 (O1A). ACC subsequently placed the advocate on a 'communications plan', which is an approach used to effectively limit the client's contact with ACC. In this case, the advocate was directed to contact the client's case manager only, who would respond to requests no more frequently than once a week.

k The client's advocate subsequently requested a digital footprint of her own sensitive claim file. That showed an ACC investigator who had looked at M's physical injury claim had also accessed the advocate's sensitive claim file.

28 In a statement to RNZ, ACC said:

> All ACC staff who access sensitive claim files do so in order to perform the functions of their job. This could be as simple as a team member reimbursing someone for a taxi or updating contact details. This activity would only involve going into part of a client's file.
>
> […]
>
> [The physiotherapist who recommended the claimant's sensitive claim be reassessed] was asked about her access and confirmed she clicked into the claim, but did not open any of the documentation in the file.

29 With respect to the staff members who accessed M's file prior to the December 2020 meeting, ACC told RNZ that 'ACC takes a holistic approach when preparing for mediation so our people can answer any questions raised during the meeting' and that staff accessed the file to create a timeline and file summary on the client and other information to 'clarify the diagnosis for any potential assessment'. ACC further noted that 'these staff were working within ACC's Code of Conduct'.

30 According to material provided by ACC for this Review:

a M and his advocate had made numerous requests, queries, complaints, and clarifications to multiple parts of ACC over a lengthy period of time.

b The table below shows the number of requests under the Privacy Act and the OIA made by M and his advocate (this does not include interactions with the Customer Resolution Team, which handles complaints from customers).

Year	No. of requests under the Privacy Act	No. of requests under the OIA
2019	1	1
2020	3	18
2021	17	93

c Generally, requests of the nature reflected in the table above involve large quantities of information and entail multiple people accessing clients' files to investigate and respond to the request.

d By way of illustration, each information request of the kind described above is handled by a minimum of four people:

i the person who receives the request;

ii the person who sets up the request on ACC's internal systems;

iii the person who undertakes a 'privacy check' of the response to the request (presumably to confirm that any disclosure of documents pursuant to the request does not inadvertently involve the disclosure of personal information beyond the scope of the request or about a person other than the requestor);

iv the person who dispatches a response to the request; and

v anyone who may be asked to advise on any stage (e.g. a team manager, member of the privacy team or legal).

e Requests that relate to reviews necessarily involve at least one other person viewing the claim from the Review Specialist teams.

f ACC's usual practice is to allocate information requests to staff according to specific tasks, which means that several ACC workers may access a client's file for purposes related to one response to an information request.

g M and his advocate also complained to the OPC on 13 July 2021 regarding requests for information made between September and November 2020, in respect of which ACC declined to provide information on the basis that such information was subject to legal professional privilege.

h On 1 September 2021, the OPC advised the client that it was satisfied that ACC had a 'proper basis to refuse the request as the information is legally privileged' and that no 'further investigation into receipt of or response to the request' was warranted in the circumstances. At that stage the OPC closed its file in relation to the client's July 2021 complaint.

i A senior ACC staff member subsequently undertook a manual check of M's files, which involved contacting those staff members who were identified on the digital footprint report as having accessed his file and asking them to confirm that their access of the file was for a legitimate purpose.

j ACC's Privacy Officer reviewed the manual checks described above, recorded reasons for the access, and concluded that all access was reasonable and legitimate in the circumstances (albeit, we were not advised how the Privacy Officer assessed the 'reasonableness' and legitimacy of access).

31 Subsequently, M's advocate filed a complaint to the Independent Complaint and Review Authority **(ICRA).** The ICRA concluded that the advocate's privacy had been breached (a breach of Right 7 of the Code of ACC Claimants' Rights) since the investigator had no lawful purpose for accessing the

advocate's sensitive claims file. This overturned the earlier finding of ACC that the access was lawful (we discuss this separate incident further in Part 6 (Access and use of client information in practice)).

32 In our view, irrespective of whether access is authorised or unauthorised, it is reasonable for clients and advocates to feel a degree of anxiety when faced with the knowledge that any file (let alone a file containing information of great sensitivity to a client) has been accessed over 300 times by 92 ACC personnel. Or, as the advocate did, that a file had been accessed in association with an investigation into another person. We identify later in this report the issues raised by this incident.

Snapchat Incident

33 On 26 October 2021, a RNZ journalist emailed ACC screenshots allegedly sent by ACC staff who were all members of a Snapchat group named 'ACC Whores'.

34 ACC subsequently identified 12 workers understood by ACC to have been members of this group (comprising ten ACC employees and two contractors) **(Snapchat Group).** Each member confirmed to ACC that they were or had been a member of the Snapchat Group.

35 These members included eight permanent employees, two fixed term employees and two agency workers. Only one of the members had been employed by ACC for more than six months before ACC became aware of the Snapchat Incident in October 2021.

36 Snapchat is an app that enables users to send content, typically a photo or video with or without captions, to others. Messages sent on Snapchat usually 'disappear' after a period (set by the sender), but any recipient can capture a screenshot. If the recipient captures a screenshot, the sender is notified. A Snapchat group enables group members to send content to all group members simultaneously.

37 According to information gathered by ACC (including the transcripts of an interview between ACC and one of the Snapchat Group members), the Snapchat Incident took place as follows:

a The Snapchat Group was established in May 2021, shortly after a group of new staff members commenced employment at one of ACC's call centres. The initial purpose of the Snapchat Group was social in nature: the members wanted to get to know each other better, to become friends. Members predominantly shared images and videos of themselves and others at social events outside of work hours.

b The content evolved over time. One member estimated that approximately 50% of the content shared within the group was non-work related (albeit, neither ACC nor the member defined what was meant by 'non-work related' in the context of the interview).

c In addition to content relating to the social lives of the members, the cohort would share content relating to their working lives at ACC. For instance, if a Snapchat Group member experienced a difficult or stressful client call, they might share that experience with the Snapchat Group by videoing themselves speaking about the call and how it made them feel.

d While ACC uses other 'messaging' platforms operationally (including Microsoft Teams and email), the members of the Snapchat Group tended to use the Snapchat Group to communicate, particularly when working remotely. At the key time in question (August to October 2021) New Zealand was under various levels of COVId-19 restrictions, meaning call centre workers, such as members of the Snapchat Group, had extended periods during which they worked exclusively from their own homes - see paragraphs 43 to 46 below.

e The membership grew over time. As new personnel joined the Snapchat Group's team at the call centre, they were added to the Snapchat Group. The majority of the members of the group were younger than 30 years old.

f Members had varying levels of involvement with the Snapchat Group — some members were described as 'very active', whilst others were 'not active at all' (although they would still receive each message).

g While all members were, at the time they were added to the Snapchat Group, working for ACC (whether as an employee or contractor), two individuals remained members of the Snapchat Group after they had ceased working for ACC.

h Some of the content shared within the Snapchat Group included information about clients.

i Subsequently, as is evident from the resulting media coverage, screenshots of content shared within the Snapchat Group were also shared with the RNZ reporter. Those screenshots show images, presumably captured through Snapchat, of ACC's claims management system, and show portions of a client's file, as described in the following table:

Approximate date content was shared	Description of content
Between 3 May 2021 and 17 August 2021	A photo of a portion of a client file showing the following file information: Took 200 ampules of nitrous at a party after sitting final essays for [...] [...] accident happen? Accident location: Auckland City Accident cause: Loss Balance/Personal Contrl The Snapchat Group member who posted this photo included the caption: 'Girl really went all out'
Early October 2021	A photo of a portion of a client file, relating to Client X, a well-known New Zealander, showing the client's email address, together with information about where and how the injury occurred.
Unknown	A photo of a portion of a client file showing the following information: How did the accident happen? Drinking and thought it was a good idea to punch a post
Unknown	A photo of a portion of a client file showing the following information: reaction to canabis***Leisure/hobby or play***Oral ingestionAccident location: Waikato District Accident cause: Loss Balance/Personal Contrl

38 ACC's investigation showed that approximately 10 images containing client information were shared within the Snapchat Group from its inception in May 2021 until 26 October 2021. These images relate to clients. ACC also determined that:

a one member of the Snapchat Group accessed the file of Client X on 12 October at 12.27pm. The member accessed the file while responding to a call made by Client X to the call centre. This staff member's access to the file was authorised;

b two members of the group shared client information;

c no 'sensitive claim' information was shared on Snapchat by the Snapchat Group;

d members of the Snapchat Group considered the Snapchat Group to be a method of sharing 'in house' information in a similar way to how information would be shared face to face when they were working in the office; and

e one member of the Snapchat Group had not completed the privacy training modules (discussed further in Part 8 (Culture)), and some had only completed them in September 2021, some months after they started working at the call centre and after they first had access to client information.

39 We were advised that ACC did not carry out checks as to whether initial access by staff to the personal information of the clients other than Client X was authorised, since ACC took the view that the screenshots referencing clients other than Client X did not include identifying information about any individual.

ACC investigation and disciplinary action

40 On 26 October 2021 — the same day that ACC was alerted to the existence of the Snapchat Group by RNZ — ACC contacted (by phone) each of the 12 workers identified by ACC as being members of the Snapchat Group.

41 On 28 October 2021 and 29 October 2021, ACC commenced an employment disciplinary process.

42 By the end of the disciplinary process, all members of the Snapchat Group had ceased their employment with ACC. Some resigned, some were summarily dismissed and those that worked through an employment agency had their contracts terminated.

Additional context — COVID-19 related restrictions

43 The Snapchat Incident took place between 3 May 2021 and 26 October 2021.

44 At 11:59pm on 17 August 2021, New Zealand entered an Alert Level 4 lockdown. On 31 August 2021, all of New Zealand (except for Auckland) moved into Alert Level 3 restrictions and then into Level 2 on 7 September 2021. On 7 October 2021, Hamilton re-entered Alert Level 3 restrictions.

45 At Alert Level 4, almost all individuals were required to work from home (with exceptions for essential workers). Under Alert Level 3, individuals were required to work from home unless that was not possible. At Alert Levels 1 and 2, all businesses were permitted to open with public health rules in place.

46 As a result, the incident that occurred in relation to the call of 12 October 2021 (discussed at paragraph 38 above) appears likely to have occurred when staff were in lockdown and working from home. This Review discusses the impacts of the lockdown and working from home on the way that staff engage with one another in Part 8 (Culture).

Issues arising from the incidents

47 The two incidents raise a number of issues relating to ACC's systems in place to collect, manage and use personal information and the organisation's culture about personal information and privacy.

48 These issues highlight tensions that push and pull two ways. In the case of the Access Incident:

a Clients are entitled to expect that the minimum number of 'eyes' will access their personal information, and that only those staff with a legitimate reason for accessing their files (or certain information in their file) will do so. This requires ACC to have clearly defined boundaries for determining who should have access and for what purpose. All ACC staff need to understand these boundaries and know what applies to them and the work they do; but also

b ACC staff, particularly call centre workers, manage multiple calls each shift with each client seeking a swift response to a personal and pressing query, preferably without being 'passed on' to a second or third ACC staff member. Providing this level of service requires ready access to client information. Requests cover a range of issues that are unpredictable. Call centre workers may need to access a wide range of different information across a large number of calls each day; and

c There needs to be regular monitoring and auditing of access so that staff are deterred from the temptation to browse any client information and clients can be reassured all access is necessary and in their interests.

49 In the case of the Snapchat Incident:

a Clients' personal information should never be shared in any format (whether face to face or online) between staff for any reason other than to further assist the client and/or their claim. Public trust in ACC requires this; and

b ACC staff must be trained and inducted into the organisation in such a way that they fully understand the significance of all personal information, the value of privacy and their obligations under the Privacy Act; but also

c Managing client demands is difficult work and can be emotionally draining and/or confronting. Frontline staff do need to decompress after some calls and there is an onus on ACC to ensure there are safe ways of doing so without breaching privacy or running counter to clients' expectations.

50 In both cases, we were surprised to learn of the significant administrative issues engaged when ACC sets out to audit access or act on complaints about unauthorised access. Addressing these issues, together with the circumstances which contribute to such high volumes of access involves an analysis of ACC's systems and processes (which we comment on further in Part 7 (Systems)).

Part 4
Legislative and regulatory framework

4 Legislative and regulatory framework

Overview

51 ACC has a duty to preciously guard the client information it collects, holds, accesses and shares not only because this is what clients would want and expect but because the law requires it.

52 This Part 4 summarises the applicable legislative and regulatory framework with which ACC must comply.

53 While assessing all law and policy applicable to ACC's management of information is beyond the scope of this Review, in order to provide an accurate picture of ACC's obligations when managing information, it is necessary to assess the broader legislative and regulatory context within which ACC operates.

54 By way of summary:

a ACC is established by the AC Act. The AC Act, among other matters, authorises ACC to collect and share injury related information. But it also dictates that ACC must only collect such information for specified purposes, one of which is providing rehabilitation, treatment and/or compensation to clients who have suffered injuries.

b The ACC Code of Claimants' Rights **(ACC Code)** establishes specific rights for claimants (and corresponding obligations for ACC), including a right for claimants to have their privacy respected.

c ACC is subject to the I PPs under the Privacy Act which govern the collection, use, retention, and disclosure of 'personal information'. The Health Information Privacy Code 2020 **(HIP Code)** establishes health information privacy rules **(HIPC Rules),** which modify the IPPs in respect of 'health information'. Among other obligations, ACC is required to protect the personal information (including health information) that it holds against misuse, and only use that information for the purposes for which ACC obtained it.

55 For completeness:

a ACC, like other crown entities, is subject to the OIA which allows individuals and New Zealand bodies corporate to ask ACC to disclose any official information it holds in its capacity as an 'organisation'. Subject to limited exceptions, ACC must provide the information requested.

b ACC has further information management obligations under the Public Records Act 2005 **(Public Records Act),** and the Information and Records Management Standard issued under the Public Records Act. Among other obligations, ACC must ensure that information is managed appropriately, and that information is protected from unauthorised or unlawful access, alteration, loss, deletion, and destruction.

c As a crown entity ACC is also subject to the Public Service Act 2020 **(Public Service Act)** which describes the principles (the fundamental features of the way in which the public service operates) and values (the necessary behaviours of public servants to maintain the integrity of the public service) underpinning New Zealand's public service. This is particularly relevant to the Board of ACC, who are responsible for ensuring ACC abides by the public service principles set out in the Public Service Act.

56 Each of these statutes, standards and codes imposes obligations on ACC as an organisation and on ACC staff as agents of the organisation. We discuss the AC Act, the ACC Code, and the privacy legislation referred to at paragraph 54 above, in more detail below.

AC Act

57 The AC Act establishes the functions, obligations, structure, and management of ACC. The AC Act seeks to enhance the public good and reinforce the social contract, by providing for a 'fair and sustainable scheme for managing personal injury'.

58 The 'framework' for the collection, co-ordination, and analysis of injury-related information is primarily established by Part 7 of the AC Act. This framework sits alongside the requirements of the Privacy Act (discussed further below) and other privacy legislation.

59 Section 279 prescribes the 'purposes' for which ACC may collect information. ACC should be mindful of these purposes, as well as ACC's obligations under the I PPs (again, discussed further below), every time personal information is collected. The purposes established by section 279 are:

a to enable a comprehensive claims database to be maintained;

b to facilitate the monitoring of the operation of the AC 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 the AC Act;

h determining the cost to society of personal injury;

i levy setting; and

j scheme management.

Code of ACC Claimants' Rights

60 The ACC Code is established under Part 3 of the AC Act.

61 The purpose of the ACC Code is prescribed by section 40 of the AC Act, namely, to meet the reasonable expectations of claimants (including the highest practicable standard of service and fairness) about how ACC should deal with them, by:

a conferring rights on claimants and imposing obligations on ACC in relation to how ACC should deal with claimants;

b providing for the procedure for lodging and dealing with complaints about breaches of the ACC Code by ACC;

c providing for the consequences of, and remedies for, a breach of the ACC Code by ACC;

d providing how and to what extent ACC must address situations where its conduct is not consistent with or does not uphold the rights of claimants under the ACC Code; and

e explaining a claimant's right to a review, under Part 5 of the AC Act, of a decision made under the ACC Code about a claimant's complaint.

62 The 'spirit' of the ACC Code is expressed as follows:[7]

> This Code encourages positive relationships between ACC and claimants. For ACC to assist claimants, a partnership based on mutual trust, respect, understanding, and participation is critical. Claimants and ACC need to work together, especially in the rehabilitation process. This Code is about how ACC will work with claimants to make sure they receive the highest practicable standard of service and fairness.

63 A claimant's rights (and ACC's corresponding obligations) provided by the ACC Code are expressed as being in addition to any other rights that claimants have, and obligations ACC has, under the AC Act, any other enactment, or the general law. Accordingly, the ACC Code does not serve to vary nor negate other statutory obligations that ACC has, including with respect to the management of information.

64 With respect to privacy and the management of information:

a As mentioned above, clause 1.3 of the ACC Code contemplates that, in order for ACC to assist claimants, a partnership based on mutual trust, respect, understanding, and participation is critical.

b Clause 1.4 of the ACC Code contemplates that ACC — in all its dealings with claimants - must ensure that its actions are consistent with and uphold the rights of claimants as provided for in the ACC Code, by applying the 'highest practicable standard of service and fairness'.

Claimants' rights

65 We summarise in the table below the claimants' rights provided by Part 2 of the ACC Code (together with ACC's obligations) relevant to ACC's collection, management, and use of claimants' information.

Right	Summary of right
1	Claimants have the right to be treated with dignity and respect.
2	Claimants have the right to be treated fairly and to have their views considered.
3	Claimants have the right to have their culture, values, and beliefs respected. This means ACC will: • be respectful of, and responsive to, the culture, values, and beliefs of Māori; • be respectful of, and responsive to, all cultures, values, and beliefs.
7	Claimants have the right to have their privacy respected. This means ACC will: • respect claimants' privacy; • comply with all relevant legislation relating to privacy; and • give claimants access to their information, in accordance with legislation.

66. In the event of a breach of the rights provided by Part 2 of the ACC Code, claimants have a right of complaint with ACC's complaint service.[8] This sits alongside individuals' right to lodge a complaint with ACC, the Privacy Commissioner and/or the Ombudsman.

[7] Injury Prevention, Rehabilitation, and Compensation (Code of ACC Claimants' Rights) Notice 2002, Schedule 1, cl 1.3.
[8] Part 3

67 If the complaints service determines that ACC has breached the ACC Code, ACC must address the wider implications of the breach by:[9]

a analysing and monitoring issues arising from the complaints process;

b identifying concerns with operational policies and processes;

c subsequently undertaking and remedying concerns associated with operational policies and processes as appropriate; and

d informing the claimant that the situation has been addressed.

Privacy law

68 Privacy law in New Zealand is primarily governed by the Privacy Act, which includes the 'pillars' of the Privacy Act: the 13 IPPs.

69 Generally, the IPPs encompass the lifespan of 'personal information' from the collection of that information, through to the use of that information (including within an organisation), the disclosure of that information, an individual's rights in respect of that information, and the circumstances in which that information should be deleted.

Meaning of 'personal information'

70 The Privacy Act governs 'personal information', that is:

a information about a living, identifiable individual; and

b including information relating to a death that is maintained by the Registrar-General under the Births, Deaths, Marriages, and Relationships Registration Act 1995 or any former Act (as defined in section 2 of the Births, Deaths, Marriages, and Relationships Registration Act 1995).

71 This definition is broad. Information may be personal information even if the individual concerned cannot be identified from the information itself, provided there is some other 'link' in information held by the agency which means the individual is identifiable. That being the case, personal information may include information that does not actually identify the individual concerned, including information that is only about an 'identifiable' individual by reason of extrinsic knowledge or information, or information that can be linked to an identifiable individual through the use of other information.

Meaning of health information

72 The HIP Code, established by the Privacy Commissioner pursuant to the Privacy Act, provides the HIPC Rules, which modify the IPPs in respect of 'health information' that is collected, held, used, and disclosed by 'health agencies'.

73 Health information in the context of the HIP Code is information to which the HIP Code applies. The HIP Code applies to the collection, use, disclosure, and retention, by a 'health agency' (including ACC), of the following classes of information about an identifiable individual:

a information about the health of that individual, including their medical history;

b information about any disabilities that individual has, or has had;

c information about any health services or disability services that are being provided, or have been provided, to that individual; and

d information about that individual, which is collected before or in the course of, and incidental to, the provision of any health service or disability service to that individual.

[9] Part 5

Application of IPPs and HIPC Rules to ACC

74 ACC is both an 'agency' for the purposes of the Privacy Act and a 'health agency' for the purposes of HIP Code (on the basis that ACC provides services in respect of health information).

75 In the context of the use of and access to information within ACC:

a the HIPC Rules will apply to ACC's use, storage, and disclosure of health information; and

b the Privacy Act will otherwise apply to ACC's use, storage, and disclosure of personal information.

76 The IPPs and HIPC Rules are intended to establish an underlying framework, which informs (but does not negate) legislative provisions that govern the holding, use, disclosure, and processing of personal information. In the context of ACC, this means that ACC's obligations under the Privacy Act should be viewed in the context of its obligations under the ACC Code, including ACC's obligation to treat claimants with dignity and respect and to respect the privacy of claimants.

77 We summarise in the table below the IPPs and HIPC Rules directly applicable to ACC's use and management of personal information (including health information).

IPP/HIPC Rule	Summary
1, 2, 3, 4	*Collection of information* ACC must ensure that: ACC must ensure that the personal information ACC holds is protected by such security safeguards as are reasonable in the circumstances to take against: • Under IPP 1, ACC only collects personal information for a lawful purpose, connected with a function or activity of ACC's business (and then only so much information as is necessary for that lawful purpose). Section 279 of the AC Act contemplates a list of 'purposes' for which ACC is permitted to collect information. • Under IPP 2, ACC only collects personal information directly from the individual client (unless ACC has the authorisation of the clients or another IPP 2 exception applies). The nature of ACC's statutory function means that a significant portion of client information obtained by ACC is from third parties (such as treatment providers). Where ACC collects information from a third party source, it must be able to establish that such collection is permitted under the exemptions to IPP 2 or HIPC Rule 2 (as the case may be). • Under IPP 3, when collecting personal information directly from individuals, ACC takes all 'reasonable steps' to ensure that clients are aware of (among other matters) the fact and purposes for which their personal information may be held and used by ACC. This means taking care to make sure clients understand the way information is used within ACC, including how information may be accessed and used internally. • Under IPP 4, to only collect personal information by a means that is lawful and, in the circumstances, fair and not unreasonably intrusive.
5	*Storage and security of information* ACC must ensure that the personal information ACC holds is protected by such security safeguards as are reasonable in the circumstances to take against: • loss; • access, use, modification, or disclosure not authorised by ACC; and • other misuse.

IPP/HIPC Rule	Summary
	Documents containing health information to which the HIP Code applies must also be disposed of in a manner that preserves the privacy of the individual concerned. The nature of the information that ACC holds is such that the safeguards in place to protect client information must meet a higher standard than those applied to information of a less sensitive nature. This involves safeguards to prevent not only inadvertent disclosures of personal information, but also organisational safeguards and measures that mitigate the risk of unauthorised access to information within ACC
9	*Retention of information* ACC must only keep personal information (including health information) for as long as is required for the purposes for which that information may lawfully be used. This obligation is subject to any statutory minimum retention periods Under the HIP Code, ACC is permitted to keep any document containing health information the retention of which is necessary or desirable for the purposes of providing health services or disability services to the individual concerned. In the case of health information to which the Health (Retention of Health Information) Regulations 1996 applies, the minimum retention period is 10 years beginning on the day after the date shown in the health information as the most recent date on which a provider provided services to that individual. In addition, section 66 of the AC Act requires ACC to keep every claim file for at least 10 years after the date of the last action recorded on the claim. For the most part, claims (and all information, files, and documents associated with that claim) are retained by ACC for up to 75 years following the last action on the file in accordance with ACC's retention policy. Therefore, ACC must be able to point to a lawful purpose for retaining such information, beyond the retention requirements of the above legislative requirements. That purpose should be clearly documented and transparently communicated to clients at the time their information is obtained.
10	*Limits on use of information* ACC must only use personal information (including health information) that ACC holds: • for the purposes for which ACC obtained that information; • for directly related purposes; or • on one of the other limited grounds of use provided by HIPC Rule 10 (in the case of health information) or by IPP 10 (in the case of all other personal information). In the context of IPP 10, ACC will be considered to have 'used' information when processing that information within ACC, including when information is shared between staff members. This means that ACC must be able to point to a lawful purpose whenever ACC staff access a client file (as well as when staff make use of information within a client file). Generally, the purposes for which ACC may use personal information will be those disclosed to an individual at the time ACC collects their personal information. Where

IPP/HIPC Rule	Summary
	ACC receives personal information from a third party (which interviewees noted was the case for a significant amount of data that ACC processes), ACC still needs to be able to establish that the purposes for which it intends to use that information are consistent with those for which the information was obtained.

Privacy breaches

78 The Privacy Act provides for a 'notifiable privacy breach' regime which requires ACC to, in the event of a notifiable privacy breach, notify the Privacy Commissioner and the affected individuals (or in some cases, give public notice).[10]

79 As we discuss in greater detail in Part 8 (Culture), this Review identified an organisation-wide narrow focus on 'external' breaches and, in some cases, a real misunderstanding amongst ACC staff of what is meant by 'privacy breach'.

80 As one interviewee put it, the average ACC worker understands a breach to mean that 'somebody has sent personal information, externally, to someone that they should not have'.

81 Another interviewee noted:

> I would say that the training at ACC focuses primarily on external breaches. I would say that, in terms of the internal stuff, there's a lot of common sense involved that they possibly rely on way too much...the information that we have about privacy focuses on externals.

82 It is therefore important to highlight that the Privacy Act defines 'privacy breach' as:

> in relation to personal information held by an agency:
>
> (a) unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information; or
>
> (b) any action that prevents the agency from accessing the information on either a temporary or permanent basis.

83 A privacy breach is broader than the unauthorised disclosure of information to a third party. A breach may involve unauthorised disclosure within ACC. For example, unauthorised access to personal information by an employee ('employee browsing') or the unauthorised sharing of client information between staff.

84 Not all privacy breaches will trigger notification requirements under the Privacy Act. A privacy breach is a notifiable privacy breach for the purposes of the Privacy Act if it is reasonable to believe that breach has caused 'serious harm' to an affected individual, or is likely to do so.

10 Privacy Act 2020, Part 6.

Part 5

Policies and procedures

5 Policies and procedures

85 This Part 5 considers the appropriateness and effectiveness of ACC's policies and procedures relevant to the management of client information and offers ways that such policies may be strengthened.

86 The policies ACC has in place reflect decisions that ACC has made about how client information should be treated. Such policies are the mechanism by which staff understand their statutory obligations and are guided and instructed as to how to comply with them.

87 To that end, ACC's policies need to be clear and easily relied on. They also need to not only reflect ACC's statutory obligations, but also ACC's clients' expectations of acceptable behaviours when it comes to how ACC will manage their personal information.

88 In short, this Part 5 concludes the following:

a **Lack of clear guidance for staff:** When read together, ACC's policies do not provide a clear and practical framework for staff about the appropriate use, collection and disclosure of client information. They do not give primacy to clients' privacy. Generally, the policies rely on staff interpreting technical and legal concepts, such as the application of 'reasonable' security safeguards. The majority of staff will not understand what this means in practice. ACC's policies should translate nuanced technical and legal requirements and principles into clear and practical steps and expectations for staff to follow.

b **Lack of regular and thorough review:** There are, concerningly, references to outdated privacy legislation throughout the documentation we reviewed, including the Privacy Policy and Code of Conduct. This indicates a lack of thorough review and update of the policies and suggests that there are no clear procedures in place to ensure policies generally remain up to date and practically applicable.

Overview

89 A fundamental tenet of this Review is that client information is ACC's biggest asset and that its management of that asset is central to how ACC operates as an organisation.

90 It follows that ACC has in place a number of policies and procedural documents that are potentially relevant to ACC's approach to privacy and the management of client information, including the following policies:

a Privacy Policy (internal facing).

b Code of Conduct.

c Media Policy.

d Integrity Policy.

e Information Security Policy.

f Information Gathering Policy.

g Email and Instant Messaging Policy.

h Use of Internet Policy.

i Telephony Policy.

91 Our impression is that a number of ACC's core policies contain gaps, such that they do not effectively inform staff about how to manage client information in a way that supports ACC to meet

its statutory obligations and to ensure that clients' privacy is protected. In particular, we have identified the following key gaps:

a The Privacy Policy, which is published in multiple forms, has not been kept updated. It lacks clear, up to date, and best practice guidance about how staff should manage client information to protect clients' privacy (see our further comments at paragraphs 98 to 116).

b The Code of Conduct requires staff to 'take all reasonable steps to protect the privacy of clients' but it provides no explanation about what that means in practice (that is, what is appropriate and inappropriate behaviours in the context of client information) (see our comments at paragraphs 117 to 123).

c The Integrity Policy includes no reference to personal information, nor does it establish that the misuse of client information would be an integrity incident (see our comments at paragraphs 124 to 131).

d ACC has no working from home or remote working policy and ACC's intranet page about working from home provides no clear and practical guidance for staff in terms of the impact of working remotely on ACC's obligations to protect client information (see our comments at paragraphs 132 to 137).

e ACC has no standalone social media policy (see our comments at paragraphs 138 to 143).

Five lines of assurance model

92 The 2012 Independent Review (discussed in greater detail in Part 8 (Culture)) emphasised individual responsibility for privacy. This was understandable, given the breach that occurred in 2011 was the result of an individual staff member's inadvertent disclosure and highlighted the importance of ensuring that staff understand the risks involved in the actions they take, even when in error.

93 However, in practice this appears to have been implemented as a 'bottom up', rather than lop down' responsibility chain. The reality of this is demonstrated in ACC's application of its 'five lines of assurance'.

94 The five lines of assurance model is a framework for the monitoring and oversight of a given policy, to ensure that risks are being managed effectively at different levels. The five lines of assurance are:

a First line: employees and managers.

b Second line: specialist team within ACC (for example Talent).

c Third line: independent assurance services (for example auditors).

d Fourth line: executive.

e Fifth line: Board.

95 In practice, at each 'line', responsibility is allocated for particular aspects of the policy and its implementation. Many of the policies describe typical activities to be undertaken by each line.

96 By way of example, under the Privacy Policy (which we discuss in greater detail below at paragraphs 98 to 116 below):

a The first line of assurance is employees and people managers. They are responsible for recognising and proactively managing privacy risks. Their activities include embedding ‘privacy by design’ into the business, undertaking regular privacy training, monitoring privacy issues, and breach reporting.

b At the second line, the privacy team has responsibility for supporting ACC in managing privacy risk.

c At the third line, assurance services provide independent information on the overall reliability of processes and performance under the Privacy Policy.

d At the fourth line, the Executive is responsible for building and maintaining privacy risk management processes. They receive regular reports on privacy as an Enterprise Risk, privacy compliance, and progress against the Privacy Maturity Assessment Framework.

e At the fifth line, the Board has overall responsibility for ensuring that privacy risk management is in place.

97 Currently, the five lines of assurance model is structured so that the lower levels of the organisation carry the greatest responsibility for privacy and the prevention of privacy breaches.

RECOMMENDATION: FIVE LINES OF ASSURANCE MODEL

R5.1: Consider a reformulation of the five lines of assurance model for the Privacy Policy, with a view to improving accountability for privacy at an executive level and above.

Privacy policy

98 ACC's Privacy Policy addresses how ACC uses personal and health information, and states that ACC is committed to managing information 'as carefully and respectfully as if it were our own'.

99 The Privacy Policy was last approved in August 2018 and scheduled for review in August 2020 (which did not transpire). In 2019, ACC moved all policies to a three-yearly review cycle, but the review of the Privacy Policy scheduled for August 2021 also did not happen. An external maturity review and a review of ACC's policies (including the Privacy Policy) was scheduled to occur when the Head of Privacy was appointed (which took place in September 2021). That review was again delayed so as to take into account the findings of this Review. The upshot is that the Privacy Policy has not been reviewed in more than three years.

100 The Privacy Policy refers to ACC's 'strong privacy culture focusing on protecting and managing personal information'. Like other documents we reviewed, the privacy policy states that ACC is 'focused on being a leader of privacy practice in New Zealand'.

101 In terms of accountability, the Privacy Policy contemplates that the Board is accountable for privacy and information management, setting clear expectations, communicating such expectations, and holding executive management to account. Managers are accountable for reporting risks to the Board. Breaches of the policy may result in disciplinary action, in accordance with the Code of Conduct (discussed further below at paragraphs 117 to 123).

102 The Privacy Policy also clearly sets out the broad meaning of 'personal information'.

103 However, crucially, the Privacy Policy is out of date. The Privacy Policy refers to repealed legislation:

a the Privacy Act 1993 (1993 Act) replaced on 1 December 2020; and

b the Health Information Privacy Code 1994 (1994 Code), also replaced on 1 December 2020.

104 Tellingly, the objective of the Privacy Policy is stated as to 'promote high standards' for managing personal and health information and to 'ensure compliance' with the 1993 Act and the 1994 Code.

105 That the Privacy Policy refers to legislation replaced over a year ago suggests that the Privacy Policy has not been reviewed in this time. There is therefore a disconnect: staff cannot be expected to

ensure compliance with privacy law as required by the policy where the policy itself does not provide an accurate summary of ACC's statutory obligations.

106 This is not a merely administrative flaw. The commencement of the Privacy Act in 2020 saw the introduction of a new notifiable privacy breach regime, which is premised on the occurrence of a 'privacy breach'. While the Privacy Policy addresses privacy 'incidents' (and other documentation provided to the Review, including in the context of ACC's internal privacy 'hub', reflects the commencement of the notifiable privacy breach regime), the Privacy Policy does not reflect the broad statutory definition of 'privacy breach'. See our further comments on the meaning of 'privacy breach' in Part 4 (Legislative and regulatory framework). The public-facing privacy policy available on ACC's website also refers to the 1993 Act. This reflects the Review's impression of staff's poor understanding of what constitutes a 'privacy breach'.

107 In addition to new requirements in respect of privacy breaches, best practice has shifted and new guidance has been released by the OPC since the Privacy Policy was last reviewed in August 2018.

108 Indeed, the organisational structure of ACC has demonstrably shifted since that last review. This is significant because, according to the Privacy Policy, the key person accountable for 'ensuring that supporting guidelines, operational measures, and monitoring' are in place is the Chief Governance Officer: that role has been disestablished for over a year.

109 While the Privacy Policy contemplates that ACC will take a 'continuous improvement approach' to privacy and 'look for opportunities to adopt best practice from domestic and international experience', it is clear on the face of the document itself that this has not eventuated. Even internal guidance documents remain out date, with reference to a 'Privacy Maturity Plan' that 'formalises' ACC's approach to improving privacy maturity between 2016 and 2020.

110 Beyond the outdated references to legislation and other documentation, the Privacy Policy is also, in the main, a summary document of the (then) legislative requirements: it summarises what the requirements of the 1993 Act and 1994 Code are, and contemplates that ACC will comply with those requirements. But little practical guidance is provided to the personnel to which the policy applies, such as what ACC's obligations under the Privacy Act actually mean for staff on a day-to-day basis. Nor does the Privacy Policy appear to align with actual practice in terms of how ACC manages client information.

111 By way of example, clause 4.6 of the Privacy Policy — which is the only section directly addressing the use of client information — contemplates the following:

> We use information to:
>
> - Assess entitlements to compensation, rehabilitation, and medical treatment.
> - Assist the evaluation of our services and performance.
> - Contribute to research into injury prevention and effective rehabilitation.
> - Ascertain levy payments and maintain the Scheme.
>
> Personal and health information is used and disclosed for the purposes consistent with the reason it was obtained, and the core business purposes of ACC. Reasonable steps will be taken to ensure personal and health information is complete, relevant, and up to date.

112 Staff interviewed for the Review recalled instances where ACC had used client information for a range of other purposes, such as for staff training (including in circumstances where techniques to protect the identity of the clients did not fully prevent staff from identifying the individual clients concerned). Such use falls outside the disclosures made to clients in ACC's public-facing privacy policy.

113 The Privacy Policy also does not set clear expectations as to what is unacceptable behaviour (other than, generally, breaches of the Privacy Policy itself). From the interviews conducted for this Review, we conclude that staff need much greater clarity about what 'use' of personal information means; what they can reasonably do (or access); and where the lines are drawn between authorised and unauthorised use.

114 Other than the brief, introductory statement about how ACC is 'committed to managing information as carefully and respectfully as if it were our own', the Privacy Policy makes no reference to how all personal information should be protected. This needs explanation since privacy is an intangible concept for most people (see our further comments in this regard at Part 8 (Culture)).

115 A policy document that merely restates legislative obligations is of limited utility, especially where that document is not accompanied by clear, regular, and targeted training, and a high level of organisation-wide privacy maturity.

116 The Privacy Policy should serve as a useful touchstone of both expected behaviours and practical guidance as to how the Privacy Act will apply. Such guidance should be informed by how ACC manages client information in practice, as detailed in the client information roadmap recommended in Part 7 (Systems).

RECOMMENDATIONS: PRIVACY POLICY

- **R5.2:** Allocate responsibility for the application, enforcement, and management of the Privacy Policy to a member of the executive team, consider how best to ensure that appropriate mandates and structures are in place to clearly drive opportunities for updates to the Privacy Policy, and put processes in place to ensure those changes can occur across all parts of ACC's business.
- **R5.3:** Review and update the Privacy Policy to reflect and incorporate:
    - changes to legislation and best practice;
    - changes to ACC's organisational structure;
    - the client information roadmap, prepared in accordance with **R7.1;**
    - clear expectations about managing client information, including providing practical guidance on what staff should and should not do to ensure client information is protected; and
    - more regular reviews (for instance, on an annual basis) and accountability mechanisms to better ensure the document remains up to date (in accordance with the processes put in place in response to **R5.2).**

Code of conduct

117 ACC's Code of Conduct **(Code of Conduct)** applies to all employees of ACC and is based on the State Services Standard of Integrity and Conduct. The introductory statement to the Code of Conduct contemplates:

> Everyone who works for ACC has an important role to play in making sure we achieve our vision, and in ensuring we maintain our reputation and standing in the perception of the public. Our actions and behaviours must be consistent with these expectations at all times.

118 The Code of Conduct was last approved in February 2020 and is scheduled for review in February 2023.

119 Staff are expected to (among other matters):

a exercise 'good judgement' to determine what action to take in any given circumstance and ensure such actions withstand scrutiny from internal and external parties;

b uphold the ACC Code (see our commentary on the ACC Code in Part 4 (Legislative and regulatory framework));

c comply with all ACC policies, processes, and procedures;

d use ACC information and property appropriately by 'being responsible for the security and confidentiality of all information';

e take all reasonable steps to protect the privacy of clients, customers, employees, and other stakeholders; and

f act within law, including the 1993 Act and 1994 Code. For the reasons outlined above in the context of the Privacy Policy (see paragraphs 103 to 109), it is concerning to see outdated references to privacy legislation, particularly in a document that establishes the core expectations for ACC personnel.

120 In terms of accountabilities and responsibilities, employees must read, understand, and follow the Code of Conduct. Managers must establish and promote expected standards. The Chief Talent Officer must monitor the effectiveness of the Code of Conduct and ensure organisation controls are in place to support the Code of Conduct. The Executive must 'model the highest standards' of the Code of Conduct and ensure those behaviours are integrated into ACC's business. The Board must approve the Code of Conduct and ensure it is consistent with ACC's strategic direction.

121 Concemingly, the only reference to client information is grouped with ACC's property, and staff's obligations are focused on ensuring the 'confidentiality and security' of that information by taking 'reasonable steps' to protect clients' privacy.

122 While the Code of Conduct references clients' rights under the ACC Code (which, as discussed further in Part 4 (Legislative and regulatory framework) includes clients' right to have their privacy respected, no specific client rights are called out by the Code of Conduct. Staff are not provided with clear guidelines about what this means in practice.

123 A policy is only one tool when it comes to setting clear expectations about appropriate and inappropriate behaviours for managing client information. Expectations need to be embedded in an organisation's culture, which should in turn drive systems choices to support good practice. But a code of conduct policy provides a useful touchstone for what is, and is not, acceptable.

RECOMMENDATION: CODE OF CONDUCT

R5.4: Review and update the Code of Conduct to reflect and incorporate:

- changes to legislation and best practice;
- clear expectations about managing client information, including inappropriate behaviours such as browsing of client files; and
- more regular reviews (for instance, on an annual basis) to better ensure the document remains up to date.

Integrity Policy

124 The Integrity Policy guides ethical actions and behaviours and applies to all employees, including temporary and casual employees as well as contractors and consultants. The policy states that it should be read alongside the Integrity Framework. Integrity is defined under the Policy as being:

> ...an agreed set of attitudes and ways of working which foster honest, ethical behaviour and work practices. ACC considers fraud,"[11] waste[12] and abuse[13] have the capacity to undermine the integrity of the Scheme.

125 The Integrity Policy was last approved in October 2020 and is scheduled for review on 20 October 2023.

126 The Integrity Policy contemplates that integrity underpins effective and trusted partnerships. In its simplest form, integrity is about doing the right thing, in the right way, even when no one is watching. People are expected to maintain the highest standards of integrity, discretion and ethical conduct when performing duties or representing ACC.

127 The Integrity Policy requires that all integrity incidents be reported to Integrity Services or Talent. Concerns are kept in confidence and anonymity is assured wherever possible. It notes that Integrity framework activities are guided by 'clear, concise, and consistent processes for reporting and declaring integrity issues'.

128 In this way, the Integrity Policy should be the backbone of ACC's callout culture. As is noted above, it requires all integrity incidents to be reported. Guidelines are given to ACC staff to assess whether their decision might result in an integrity incident, including questions such as 'would your decision be lawful and in line with our policies and standards?' or 'what would your reaction be if your decision appeared in the media or social media?'.

129 Importantly, the guidelines given to staff and the definition of integrity include no reference to personal information or the fact that misuse of personal information would be an integrity incident. This is of concern as personal information is ACC's greatest asset and misuse of personal information is therefore one of ACC's greatest integrity risks. Any misuse of personal information poses a significant risk of media attention (as occurred with the Access Incident and the Snapchat Incident). Such attention risks eroding trust in ACC and undermining the social contract it represents.

130 Another concern identified by the Review is discussed further in Part 8 (Culture), which considers the fact the whistle-blower in the Snapchat Incident alerted media rather than raising the incident internally in the first instance. In Part 8 (Culture) we also address the fact that very few reports of incidents involving misuse of client information had been raised using the framework established under the Integrity Policy. In our view, this highlights that the Integrity Policy is not fit for purpose and not widely used or understood by the organisation.

131 We make recommendations to address these two gaps below.

RECOMMENDATIONS: INTEGRITY POLICY

- **R5.5:** Review and amend the Integrity Policy with a view to ensuring that:
  - it is clear to ACC staff that misuse of client information is an integrity incident;
  - misuse of client information is defined broadly; and
  - staff understand activities such as browsing of client files would be considered an integrity incident for the purposes of the policy.

[11] Defined as 'any unlawful act or omission made with an intent to gain advantage for yourself or another'

[12] defined as 'any careless act or omission made consciously or otherwise to gain an advantage contrary to policy, practice, or procedure'

[13] defined as 'any negligent act or omission that results in an advantage for yourself or another through abuse of policy, practice, or procedure.'

- **R5.6:** Consider how the Integrity Policy can be strengthened so that it is the `backbone' of ACC's callout culture and so that ACC can be sure that:
    - staff are made aware of the policy and the processes contemplated by the policy (including so that staff are generally aware of what they should do if they come across an integrity incident);
    - all integrity incidents are reported under the policy and staff are cognisant of the importance of raising incidents internally to give ACC the ability to put matters right; and
    - staff are empowered to use the policy and given confidence that their reports will be taken seriously.

Working from home policy

132 ACC does not currently have a working from home or remote working policy. In its place there is guidance on ACC's intranet for staff that work from home. The intranet page states:

> We want to do flexible working right at ACC. Focusing on what we do for our customers and New Zealand, while we improve the lives of our people, will give us more opportunity to maximise our wellbeing and successfully manage commitments in and outside of work.
>
> In considering working from home or remotely we must: do right by our customers

133 No further guidance is provided on that intranet page on how ACC can 'do right by its customers' while working from home (although the page does contain links to other pages).

134 It appears that ACC staff are required to sign a declaration and be signed off by their team leader to implement a formal working from home arrangement. The declaration asks staff to confirm that they have read guidance on how to keep ACC information safe, but there is no information about how to protect privacy and ACC information on the main remote working page. The focus instead is on 'doing right by our people' which is about doing right by ACC staff, for example, by ACC welcoming 'flexible working requests from a cultural, faith and/or disability perspective.'

135 The intranet page guidance appears to apply only to formal requests for flexible working — for example, a staff member who wants to regularly work from home one day per week for childcare or other reasons. Reviewing the information on the intranet page is embedded into the process of making a formal request.

136 This means that where staff find themselves working from home due to unexpected circumstances (for example, under a lockdown or, as happened recently, as a result of protests at Parliament), they are not necessarily required to review the intranet guidance or sign any declaration. It also appears that staff who work from home in an ad hoc manner, for example when a tradesman is visiting, would similarly not be captured by the requirement to sign a declaration.

137 A standalone policy would be able to apply to all ACC staff working from home, for whatever reason and no matter how long. It would also enable ACC to put in place clear rules and requirements for how staff can protect personal information while working from home, and how important that is.

RECOMMENDATION: WORKING FROM HOME POLICY

- **R5.7:** Assess the impact on staff of working from home, particularly for frontline staff, and consider what additional measures can be put in place to ensure staff have a safe and secure way to stay connected, including the opportunity to debrief safely.
- **R5.8:** Introduce a working from home policy that includes (at a minimum):
    - clear expectations as to how personal information should be protected while working from home, for example, working from a separate room from other members of the household where possible, limiting the use of paper documents used at home, not working near windows or high traffic areas, ensuring all calls are taken in private and so on;
    - a broad application to all ACC staff who work from home or at another location, whether via a formal arrangement, in an emergency or on an ad hoc basis;
    - a clear requirement that only ACC approved devices should be used when working from home; and
    - guidance for staff on what communication channels should be used when working from home when discussing client information.

Social media policy

138 As set out above at paragraph 90, ACC has a Media Policy, an Email and Instant Messaging Policy, a Use of Internet Policy and a Telephony Policy.

139 The only one of these policies that currently refers to social media is the Media Policy, which only refers to it from a media angle; that is, it states that ACC allows employees to express their own opinions in their own time on social media channels including liking, sharing or engaging with ACC's social media communications. However, they must not represent ACC in any form. Any questions directed at employees on social media should be passed on to official ACC social media accounts. Doing so protects ACC and the employee.

140 The lack of a standalone social media policy is a clear gap, particularly in light of the sharing that took place on Snapchat during the Snapchat Incident.

141 ACC cannot prevent its staff from using social media (or, more broadly, their own personal devices, for example text messaging on their personal phone) to communicate with one another. As noted in Part 8 (Culture), informal social media channels are useful for staff to stay in contact during lockdown or as a backup if work systems are down. However, it can and should implement a policy that puts in place clear rules and guidelines around appropriate use of social media and personal devices where that use occurs at the intersection of work and personal life.

142 Our analysis of the information gathered by ACC during its own investigation into the Snapchat Investigation showed that the staff that shared information appeared to be under the (mistaken) impression that the sharing they did wasn't wrong, because they were 'only' sharing information with ACC co-workers. A clear social media policy may go some of the way to ensuring that similar incidents do not occur in the future.

143 Another gap identified by this Review is the fact that staff may not understand the OIA and Privacy Act can apply to messages on personal devices. When interviewed, one call centre staff member (who had acknowledged that they used social media to communicate with her colleagues) said that they did not have a great understanding of the OIA. Their understanding was limited to the fact that a client could request their personal file. It was apparent from that interview that ACC had not given its call centre staff the training or knowledge they require to properly understand how information

legislation applies to messages shared on social media and other platforms such as Microsoft Teams.

RECOMMENDATION: SOCIAL MEDIA AND USE OF PERSONAL DEVICES POLICY

R5.9: Implement a social media policy that includes at least the following:

- a clear and comprehensive statement that client information should never be shared on social media or on a personal device, even if anonymised and even if the sharing is only with other ACC staff members;
- an acknowledgement that social media channels can be legitimately used by teams and groups of staff members, while also putting in place clear guidelines setting out what is and isn't acceptable use of these channels;
- guidance to ensure that staff are aware that any work related information shared on personal devices or social media is discoverable under the OIA and Privacy Act; and
- a preference that staff who are provided work devices use these for work discussion wherever possible (for example, if there is a need to text one another they do so on their work device rather than their personal device), and guidance for staff that do not have work devices that these should not be used for work related discussions unless absolutely necessary.

Part 6

Access and use of client information in practice

6 Access and use of client information in practice

144 Client M, who is in a dispute with ACC, engages a friend to be his advocate. Incidental to that dispute, the advocate requests a digital footprint from ACC to see how many ACC staff have accessed her file, including her sensitive claims file.

145 The digital footprint shows that an investigator from ACC's Integrity Services Unit, who was investigating M, had twice accessed the advocate's sensitive claim.

146 The advocate sought an explanation from ACC for why the investigator viewed her personal information, when she was not the subject of any investigation.

147 ACC responded that the investigator had opened the advocate's file 'as it was relevant to' the review of M's claim, that there are no notes in the investigation file about the access and that the investigator no longer worked for ACC.

148 Dissatisfied with this response the advocate formally complained under ACC's Code of Claimants Rights. ACC dismissed her complaint that her privacy had been breached, instead finding that the investigator had accessed her personal information 'for the purpose of investigating', which was an authorised purpose. There was no available information to indicate the investigator accessed her sensitive claim file for any other reason, ACC concluded.

149 The advocate exercised her right of review to the IRCA which found ACC breached Right 7 of the Code of Claimants Rights (the right to have privacy respected).

150 The experience of client M's advocate highlights in sharp relief some concerning issues:

a *Permission to access* — the investigator accessed the file of a client who was not the subject of a current investigation. He should have asked himself, prior to accessing the advocate's file, 'Will I be using the personal information in this file for the purpose for which ACC collected it?' Or more simply, 'Do I need to look at this? Am I authorised to do so?' The IRCA concluded the investigator did not need to look at the advocate's file to complete his investigation into M.

b *Respect for the type of information* — the investigator looked at the advocate's 'sensitive claims' file. ACC assures clients that this information is meant to be accessible to only a limited number of eyes. The IRCA said access should be allowed 'only in the rarest of circumstances'. That threshold was not met here (we note that in response to this example ACC has removed the ability for investigators to access sensitive claims files).

c *Poor auditing processes* - ACC's review of the investigator's actions were hampered by the lack of effective monitoring tools. The investigator was not required to justify access to the file and no electronic note was left on the system which showed why he did, or exactly what parts of the file he looked at. Only the fact of access having occurred was recorded.

d *High trust default* — in the absence of any extrinsic evidence as to why the investigator would have looked at the file, ACC's Integrity Unit concluded he must have been investigating, which IRCA described as 'supposition and reasoning after the fact'. In essence, ACC's position was to trust that access was authorised unless provided with evidence that it was not. This effectively puts more weight on supporting the organisation than protecting client personal information. The default position should be that all personal information must be protected.

151 Lastly, following receipt of the IRCA decision ACC's privacy team took the view that a breach of Right 7 of the Code of Claimants Rights is not a breach of the Privacy Act. On the facts established by the IRCA in this case, that is not correct. Unauthorised accessing of personal information is a breach of IPP 5 (storage and security) and IPP 10 (limited use).

152 This Review has set out this case at some length, to provide a practical example of both the systems and culture gaps we identify in Part 7 (Systems) and Part 8 (Culture).

Part 7
Systems

7 Systems

153 The systems and processes that both clients and staff interact with daily are the tools which allow ACC to fulfil its part of the social contract with New Zealanders. To that end, they need to be easy to use, protective of each individual's personal information, transparent, and well monitored.

154 In short, this Part 7 concludes the following:

a **Information roadmap:** There is no clear roadmap setting out how client information is received, processed, used, and destroyed within ACC. Both clients and ACC staff would benefit from this being clearly defined. See our further comments at paragraphs 165 to 196.

b **Open gate access:** ACC's systems operate on 'open gate' access model in the case of most claims, whereby any ACC worker with access to a system has access to all client files. Such open gate access is accompanied by a real risk of inappropriate access to client information within ACC. See our further comments at paragraphs 197 to 234.

c **Lack of monitoring and auditing tools:** ACC's monitoring and auditing processes are inadequate. ACC does not have tools and functionality to support the regular and granular monitoring and auditing of staff access to all client information, in such a way that reflects best practice. See our further comments at paragraphs 235 to 253.

d **Transparency:** There is a disconnect between clients' expectations about how their information will be treated and how ACC actually handles that information. Some of this disconnect comes from the systems and processes that ACC uses to receive and process client information. It is incumbent on ACC to clearly explain to clients how their information will be used. See our further comments at paragraph 192.

e **Policy settings:** To the extent that gaps exist in the operational management and monitoring of access to and use of client information, these reflect policy decisions. ACC has developed an operational default setting which does not elevate protection of client personal information as a priority.

Overview

155 ACC faces a formidable task: its role means it acts as kaitiakitanga of a sensitive and significant dataset, that is, the personal information of anyone who has made a claim to ACC having suffered an injury in an accident or as a result of a crime. It processes huge quantities of information daily: ACC received approximately 2.27 million new claims in the year 1 July 2020 to 30 June 2021. Every claim involves ACC's receipt of personal information about clients.

156 Managing that information flow, and responding in a timely way to client requests, is demanding and can sometimes be stressful, with call centre workers at ACC's Dunedin and Hamilton call centres at the sharp end of the operation.

157 The responsibility that accompanies this is well understood by most of the ACC personnel interviewed for this Review, not least due to the significant operational and systems-based changes introduced by ACC to address the recommendations of the 2012 Independent Review.

158 As discussed further in Part 8 (Culture), our overall impression is that, in the wake of the 2012 Independent Review, ACC implemented a number of crucial measures and systems to prevent the inadvertent disclosure of personal information to third parties. It is without question that the findings of that earlier Review were taken seriously by the organisation and that the Review itself generated a

deep concern and sensitivity to breaches of personal information that involve the unauthorised disclosure of information to third parties.

159 In addition, ACC has clearly prioritised ensuring that client information which is categorised by ACC as being sensitive is appropriately locked down and accessible only to a subset of ACC staff. It was clear from our interviews with a sample of those persons with access to sensitive claims that the burden and responsibility that comes with being granted access to these claims was both understood and respected by the sensitive claims unit.

160 However, almost all of the ACC personnel we interviewed for this Review either identified or agreed that gaps exist in ACC's systems that serve as a barrier to ACC meeting and exceeding the expectations of the public when it comes to the handling of all client information within ACC.

161 The impression of this Review is that ACC has taken a 'systems first' approach to solving privacy related problems identified by the 2012 Independent Review and, at the same time, implemented changes according to a narrow definition as to what constitutes a privacy risk. This has resulted in policy and systems asymmetry, whereby there are systems safeguards to prevent a repeat of the 2011 privacy breach, but there are no parallel safeguards to prevent other types of privacy breaches.

162 Systems are a manifestation of an organisation's privacy culture; if there are no safeguards to prevent other types of breaches that is because there are gaps in ACC's overall privacy settings and culture. Addressing the systems gaps identified by this Review requires ACC to first shift its privacy culture, as identified by Part 8 (Culture).

163 In particular:

a There is a balance to be struck between ensuring operational efficiency and protecting individuals' privacy rights. It is not clear to us that ACC has struck this balance fairly. The organisation has undergone a sustained period of change to improve efficiency and responsiveness but this has not been matched with a similar focus on protection of privacy (notwithstanding the changes made in response to the 2012 Independent Review).

b In maximising responsiveness, ACC has adopted a 'high trust' access model which permits all staff working at a frontline operational level open gate access to all clients files, except for:

i **Sensitive claims:** these are claims relating to physical and mental injury suffered as a consequence of a criminal act, primarily sexual abuse or sexual violation. As at January 2022, 28,074 sensitive claims were active. From 1 July 2020 to 30 June 2021, 13,266 clients lodged sensitive claims with ACC. As of January 2022, 865 staff have access to these client files. This is a significant reduction in the number who had access in 2021.

ii **VIP clients:** these are claims filed by individuals classified by ACC as very important persons (such that general access to their information would be inappropriate or a security risk). They include senior politicians and celebrities (inclusion in this category of claims may only be temporary). As at January 2022, there were eight VIP clients with active claims.

iii **Remote Claims Unit (RCU) clients:** this is a group of individuals who have previously been categorised as posing a risk to ACC personnel and therefore require an additional level of security. Only selected staff are delegated to deal with these clients. As at January 2022, there were 218 RCU clients with active claims. 262 RCU claims were active.

iv **Staff files:** every claim by every ACC staff member or contractor has restricted access settings. As of February 2022 only 82 staff have access to these claims, down from 168 in 2021. The recent Improvement Initiatives identified errors in how staff claims had been loaded into EOS, meaning not all staff files have been restricted.

c Open gate access is accompanied by risk, since all staff with open gate access to client information can, in theory at least, access all information held in an individual's file, whether or not access to such information is necessary to allow the staffer to respond to a client request. Such risk can be managed and mitigated by a combination of:

i staff having very clear guidance on what they can and cannot access; and

ii regular and rigorous monitoring and auditing.

d There is no roadmap available which clearly sets out how ACC intends to collect, manage, disclose and destroy personal information and no clear or accessible policy on what factors justify access to personal information.

e The systems and processes that ACC has in place do not support ACC to safeguard all categories of client information from inappropriate internal access and use, in the way expected of any agency holding such sensitive personal information. ACC also has work to do in order to fully realise and articulate the client information 'journey' within ACC for both staff and clients.

f The systems that ACC relies on to manage personal information contribute to the disconnect between clients' expectations about how their information will be treated and how ACC actually handles that information. It is not unreasonable for individuals to be surprised when they learn about how many personnel have accessed their information held by ACC. It is incumbent on ACC to ensure that it takes all reasonable steps to ensure individuals are aware of how ACC manages their information, and how many ‘eyes’ might legitimately access a file.

g There are steps ACC can take to codify and explain the client information journey, from collection to destruction.

164 We have not, within the course of this Review, sought to traverse all aspects of ACC's information management, nor to form a view as to why systems and processes may have been designed in a particular way. Similarly, because of the organisational structure of ACC, we have concluded it would be beyond the scope of any one team (let alone any individual) to have addressed the issues identified. For this reason, our commentary should not be read as a criticism of any one person or team within ACC.

Client information management

Overview of client information

165 The term 'client information' in this Review is intended as an umbrella term to generally describe all information (including files, data, and documents) held and processed by ACC in connection with the receipt, assessment, and management of claims.

166 Such information includes information falling within the meaning of personal information. For more detail on personal information, see our further comments on the legislative and regulatory matrix applicable to ACC and its handling of personal information in Part 4 (Legislative and regulatory framework).

167 ACC receives and processes an extraordinarily significant amount of information. Each claim refers to the individual circumstances of an individual (usually a New Zealander, but not exclusively so).

168 While the majority of claims received by ACC are quickly resolved through an automated process (described further below), even the most straightforward claims involve ACC's receipt, processing, and retention of a sensitive dataset about the health and activities of each individual. The volume of claims means the range of client information managed by ACC is vast. At a very high level, information handled by ACC may include the following categories of information:

a basic contact and demographic information;

b financial information;

c employment information;

d health information, including a client's medical history beyond the specific injury for which entitlements are sought;

e information about a client's mental health; and

f contextual information in respect of an injury or client, including what activities they participate in, information about their family situation and/or support and information about criminal events in which they have either participated or been a victim.

169 Some of this information will be in the public domain, some of it will be tightly held by the individual concerned. Equally, some individuals will feel more strongly protective about the information they share with ACC, irrespective of how others regard the sensitivity of that information. It is normal for people to have different tolerances about how much information they share and/or wish to be known.

170 ACC's primary client management system is the FINEOS software programme (referred to by ACC as **EOS).**

The client information journey at ACC

171 From the outset, one aim of our Review was to understand the way ACC manages client information from the moment it collects and/or receives the information to the time it destroys it. We refer to this as the client information journey. A very high level overview of this Review's understanding of the client information journey at ACC is set out in **Schedule 2.**

172 Given the importance of managing personal information to ACC's core role we expected to find a clearly articulated roadmap setting out this journey which would be available to all staff and clients (if requested). Alongside that, we expected ACC would have established clear guidelines for determining who has access to what information and for what purpose.

173 In fact, nobody was able to provide us with a thorough and exact picture of how information is received, managed, used, disclosed, retained, and then destroyed. Everyone interviewed understood what access rights they had to information in order to fulfil their particular role but they could not provide a complete description of the client information journey, and no document (or roadmap) setting out that journey appears to exist. Likewise, no guidelines describing the circumstances in which personnel should or should not access client information in the course of their role were available. Our further commentary on the open gate nature of ACC's client information management systems is set out in paragraphs 197 to 234 below.

174 The impression of this Review is that the systems and processes used by ACC to receive and then process client information throughout the client information journey means ACC manages client information in a way that is inconsistent with clients' reasonable expectations as well as ACC's statutory obligations.

175 Before we address this point in detail it is important to set out recent changes in how ACC manages claims since this has an impact on how personal information is both accessed and used.

Next Generation Case Management

176 In 2019, ACC undertook a significant and organisation-wide review of its systems and processes through the introduction and roll out of Next Generation.

177 The transition to Next Generation across all ACC sites occurred gradually, with five 'tranches' rolled out from September 2019 to September 2020.

178 The scope of this Review does not extend to assessing the Next Generation methodology, nor the suite of documentation, papers, and context for the Board's decision to implement Next Generation. However, the implementation of Next Generation was the largest people, technology, and process change in the history of ACC, involving the migration of over 90,000 claims and impacting approximately 2,000 staff. The context of the implementation — and consequences — of Next Generation is directly relevant to this Review.

179 Next Generation was intended to enable ACC to be more responsive, easier to deal with, and more transparent. The premise of Next Generation is to treat clients as diverse individuals with different needs, based on their injury and/or circumstances (rather than focusing on the type and expected duration of the injury). ACC's objective was to focus its resource where it could have the greatest impact for customers, achieve greater consistency, and remove complexity for ACC's internal processes.

180 One major change introduced by Next Generation is that clients are triaged based on their needs, and may transition between levels of support as the complexity of their claims change and they need more or less assistance from ACC. Next Generation introduced four core 'teams' of client interaction referred to internally as 'Enabled', 'Assisted', 'Supported', and 'Partnered'. At a high level:

a 'Enabled recovery' is where the client will primarily manage their own recovery using ACC's self-service tool, MyACC, to select services and request support. Clients in 'enabled recovery' are not assigned a dedicated case manager so if they call ACC for any reason, they could be managed by any call centre worker on duty at that time. An example of a client who may receive this level of engagement is an office worker with a fracture, who can still work most of the time.

b 'Assisted recovery' is where the client will primarily manage their own recovery, but ACC will contact the client if there is something specific to discuss (for instance, where additional services are required to progress recovery). An example of a client who may receive this level of engagement is a teacher with a dislocated shoulder who may need additional services, such as help travelling to and from work.

c 'Supported recovery' is where the client is assigned a dedicated ACC contact who supports their recovery, for instance, to manage multiple treatment providers and additional services as required. An example of a client who may receive this level of engagement is a farmer with a disc-prolapse, who receives support from multiple treatment providers possibly over a longer time period, and who is recovering while working in a challenging work environment.

d 'Partnered recovery' is where the client is assigned a dedicated ACC contact, and it is anticipated that the client will need support for an indefinite period due to the complexity of their injury and need for (potentially) lifelong support and partnership. An example of a client who may receive this level of engagement is a client with paraplegia, who requires expert support to coordinate specialised services over a long period.

181 In addition, Next Generation introduced:

a Administrative teams to undertake tasks that previously accounted for 40% of a case manager's time (for instance, loading reports and medical certificates, arranging assessments, and arranging referrals for supports).

b Technology enhancements which were intended to provide a better user and client experience, including:

i Salesforce as the 'system of engagement' for ACC personnel, enabling team members with the required skill to be directed to specific tasks, which was intended to facilitate greater visibility of workflow and speed up response times.

ii MyACC, a customer-facing platform that enables ACC clients to manage aspects of their claim in their own time from their own devices.

182 Next Generation also introduced a 'Role Mapping Dictionary', which sets out the correct level of access to EOS functions — including access to sensitive claims files - for staff, who are expected to check the dictionary to ensure they are requesting the correct access for their role type. However, interviewees we spoke with were unfamiliar with the operation (or indeed existence) of such a Role Mapping Dictionary.

183 Information provided to us for the purposes of this Review suggests that the privacy team was involved in and supported the design, development, testing, and rollout of the Next Generation model, including by completing a 'privacy threshold analysis' for the testing stage of Next Generation from 2016 to 2018 (prior to the confirmation of a 'blueprint' for the model in 2019), attending and informing design sprints; contributing to training programmes and the development of new operational procedures; and delivering privacy training directly to new staff.

184 The privacy team also completed a privacy impact assessment (PIA) in respect of Next Generation. That PIA was undertaken while ACC was already in the process of rolling out the first 'tranche' of Next Generation across the organisation (in September 2019) and some months after the 'blueprint' of Next Generation was developed in July 2019. (We would have expected any privacy assessment to take place prior to the confirmation of the blueprint and the commencement of the system roll out.) That PIA identified a number of risks, including:

a that the influx of new and temporary staff unfamiliar with the breach of 2012 or 'the strong privacy culture within ACC' might have a less vigorous approach to information management; and

b that the distributed work model for staff in the Assisted Teams risked leading to a reduced sense of accountability for individual client outcomes, which could in turn lead to a less rigorous approach to information management.

185 With the exception of risks pertaining to sensitive claims, the vast majority of the risks identified in the PIA were coded as 'minor'. This indicates a misunderstanding about ACC's obligations under the Privacy Act. For example, 'a less rigorous approach to information management' may still constitute a breach of privacy in certain circumstances. It also indicates that ACC considered sensitive claims information was afforded more protection under the law. But all personal information requires protection and compliance with the Privacy Act, the I PPs and the HI PC Rules.

186 Nonetheless, the PIA conducted in respect of Next Generation identified privacy risks which ACC has opted to tolerate.

187 ACC conducted a review of Next Generation in April 2022 and concluded that — while the Next Generation PIA articulated risks pertaining to the implementation of Next Generation — the impact of a significant change management programme on privacy management was not assessed. Indeed, some frontline leaders observed a deterioration of what ACC viewed as a 'strong' privacy awareness culture which ACC considers may have contributed to an increase in breaches.

188 See our further comments in Part 8 (Culture) regarding interviewee's mixed perceptions of the effects of Next Generation from a privacy perspective.

189 Next Generation is now the established system of claims management and the privacy risks identified by ACC's privacy team have manifested as reality.

190 By way of example, the significant changes to ACC's processes introduced by the Next Generation model (discussed in paragraphs 176 to 187 above) mean client files are viewed by many different ACC personnel over the lifetime of a claim and certainly more than was previously the case. Workers respond to 'tasks' across multiple claims, rather than as dedicated case managers. (There are still dedicated case managers, but they are reserved for more complex or long lasting claims.) The Access Incident (described in Part 3 (Overview of Snapchat and Access Incidents)) is an example of how widespread access can be a cause for concern and distress for clients, even if and when such access is ultimately determined to be legitimate.

191 But the Review identified other systemic issues as well:

a ACC obtains client information from a range of sources, not just the injured individuals in whose name a claim is filed. Third party providers - such as GPs, nurses, physiotherapists, counsellors, psychologists — provide forms, files and supporting information to ACC. ACC is unable to control the types of information that it receives from third party sources — one issue identified by many interviewees was that ACC is frequently viewed by treatment providers as a repository for all information about a particular patient, whether requested by ACC or not. Said one interviewee:

> If you're looking at a claim that is quite a few years' old and you need to do a large request for medical notes. Often the GP will just send through all of the medical notes from those five years instead of just the injury related stuff. So then what would happen is before you sent out the information (to the healthcare provider who was to treat the client) you would take out only the stuff that is relevant, but there would still be a record of the other information in the documents tab. It is still being held by us.

ACC reported that it has implemented systems to identify and delete or return information that is not necessary for ACC's purposes (although staff interviewed did not appear to know of this). In any case, even the receipt of such information poses operational issues for ACC, given the quantity of claims. It was not clear to us that ACC has developed policy guidance around this issue, such that would put all providers on notice about their obligations to limit disclosure of personal information.

b Interviewees also identified that ACC has relatively little control over the form in which it receives information — despite significant work undertaken by ACC to move its systems and processes into a primarily digitised format, many interviewees noted the surprisingly large quantity of information received by ACC in the post or by fax. Information received in this form will usually require more handling, and therefore more people being required to look at it. Double-handling of significant amounts of information is inevitable with this model, as is the retention of personal information that is unrelated to ACC's management of a particular claim.

c At times, ACC will aggregate and 'scramble' information on EOS for use in data analysis in accordance with section 279(a), (b), (c), (d), and (g) of the AC Act. This is specifically provided for in the AC Act and allows the organisation to better administer the scheme by better understanding things such as injury causes and recovery trends. Aggregated and scrambled information is also used internally for training purposes. A concern noted by participants was that such 'further use' is frequently unsupported by a privacy-based control process (such that identifying information about clients is sometimes available). This was confirmed by ACC's Improvement Initiatives, which noted that of the claims files provided to data specialists (to develop and test technology changes and enhancements) 'some' had the identifying information 'obfuscated so individuals cannot be identified'. We can see no justification for any claims being handled by the development and testing team at ACC containing any information that could identify a client. It is concerning that publication and/or use

of personal information in this way has not been identified as a risk and processes put in place to ensure it does not occur in future.

d There are some circumstances where access to client information is not directly related to the management of a client's entitlement or recovery, albeit nevertheless for a lawful purpose.

ACC's Government Engagement team frequently handles requests under the OIA and/or by the Health and Disability Commissioner which require consideration of claim-specific information. Again, it is not evident that clients understand that ACC personnel beyond those directly managing their claim may be authorised to have access to their information.

e The basis for ACC's retention of client information (for 75 years following the last action on a file) is not clearly justified nor understood by the organisation. Under IPP 9 of the Privacy Act, ACC is required to only hold personal information for so long as it has a lawful basis for using that personal information (see Part 4 (Legislative and regulatory framework)). We were concerned that none of the interviewees were able to identify a specific statutory requirement, nor organisational or operational purpose, to retain this information for such a significant period of time. Again, it is not evident that ACC's retention of client information is explained to clients.

192 While each of the above examples of ACC's approach to managing client information may have arisen from a genuine operational need, ACC has a responsibility to ensure that it is transparent about the purposes for which it holds and uses personal information, not only because ACC is required by legislation to do so (including under IPP 3 and IPP 10), but also because clients are entitled to expect this degree of transparency about issues that directly affect them.

193 It is also implicit in the obligations imposed on ACC under IPP 5 (storage and security) and IPP 10 (use of information) that the only ACC personnel authorised to access a client's personal information are those who are required to do so *to assist the client with their claim and/or recovery.* It was not evident that all interviewees fully understood this basic and necessary connection between access and the purpose for access. The 'many eyes on a file' approach, which is inevitable under the Next Generation model of claims management, potentially dilutes any connection between the reason why the personal information is held and accessible and a worker's immediate task at hand (as ACC's privacy team identified at the time the model was being rolled out).

194 In order to understand how to protect personal information collected, held and managed by ACC, it is crucial that the organisation has an accurate and comprehensive roadmap of the client information journey within ACC.

195 As summarised by a person interviewed for this Review:

> There [is] no one person who could articulate the environment [of client information]. Well, that's the key starting point for me. What is the footprint? Where does [client information] go? We can understand the systems, the people, the culture, the processes we need to wrap around it all — but [the map] is just not there.

196 A client information roadmap would clearly set out expectations and obligations for both ACC staff and for clients.

RECOMMENDATIONS: CLIENT INFORMATION MAPPING

- **R7.1:** Undertake a comprehensive client information mapping exercise, for which an executive team member is responsible, for the purposes of creating a clear, complete, and accurate overview of how client information is managed within ACC, from the point of ACC's collection and receipt of that information through to its destruction. That map should remain 'live' and subject to regular review, particularly where and when new systems are introduced

- **R7.2:** With reference to the client information map prepared in accordance with **R7.1,** ensure that disclosures made to clients about how their information is managed are accurate, such that ACC's approach to client information (including the circumstances in which a client's file may be viewed by ACC personnel) is clearly understood by clients. Consider introducing a 'customer facing' version of that roadmap.

Permissions and access

Overview

197 As noted at the outset, we consider it entirely reasonable for ACC clients to expect that as few ACC staff as practicable ever have the opportunity to access their personal information. The number of potential accesses to a client's file will depend on a range of factors including, but not limited to, the nature of the client's injuries and the time required to engage with ACC during recovery and rehabilitation and the complexity of their claim. However, even for the most complex claims, it is evident that much of the contact between the client and ACC personnel may only require staff accessing limited parts of the client's file.

198 Who can or should be able to access which file or even which sections of a file are matters related to ACC's policy approaches to provisioning and access (discussed in paragraphs 200 to 203 below) as well as permissions (discussed in paragraphs 217 to 234 below).

199 In our view, ACC's current approach to access management engages the following issues:

a While ACC has in place a 'permissions' process to grant only certain persons access to EOS, ACC has no clear policy governing who, and in what circumstances, access to EOS will be granted. Subsequently, we were unable to conclude with any certainty that ACC's existing processes enable ACC to comfortably establish that only those who *require* access to EOS are granted access to the system.

b ACC does not have transparent access definitions or thresholds. In the absence of these it is unclear which roles require what level of access to client personal information. All ACC personnel should be able to see what access rights they have been granted and for what purpose.

c Open gate access is granted to all call centre staff as soon as they commence employment and even before they have completed privacy training. There are operational reasons for this; call centre workers deal directly with ACC clients and need (some) access to respond to their inquiries. ACC places a high level of trust in these workers to both understand their obligations under the Privacy Act and to abide by them.

d ACC does not maintain an up-to-date role map: As personnel move within ACC (and particularly in light of the restructures and reorganisations occurring in the business), there is a risk of 'slippage' in terms of identity and access management. The quarterly review process is aimed at mitigating such risk, but ultimately relies on management regularly and accurately completing the role checking review (and understanding, without further guidance, when access is and is not appropriate).

e Access remains assigned after it is no longer required or justified (due to personnel changing roles). Again, to some extent this issue is addressed by ACC's existing access checking processes. However, since that process is undertaken on a quarterly basis (and heavily relies on management staff), it is difficult for ACC to satisfy itself that only those who need access have access at any one time.

f The policy of limiting access to certain types of client files through categorisation is prudent and necessary. But the description of certain files as 'sensitive claims' has, over time, created a false

impression among ACC personnel that other general claims do not contain sensitive information and/or that privacy protections apply less rigorously to general claims. This is a significant risk.

g No one person has responsibility or oversight for access to EOS generally. See our further commentary on the allocation of responsibilities in Part 8 (Culture).

Current approach to provisioning and access

200 ACC personnel access client information through EOS by simply logging into the system. The version of EOS used by ACC is integrated with Azure Active Directory (Azure AD). This means that EOS user accounts are automatically created, based on predefined 'groups' of personnel defined by ACC within Azure AD (rather than by an administrative user manually creating each user account).

201 We understand that in the case of a new starter, an individual's role description will trigger the creation of a user account within the relevant Azure AD group, such that the user's account is configured to provide access to EOS. However, we were unable to clearly ascertain the process for such provisioning, nor the parameters of when such access is considered 'necessary' for the specific responsibilities of a role.

202 ACC undertakes a quarterly review of its EOS permission settings as part of a broader regular check on systems access. At a high level, that systems check process is designed to work as follows:

a a systems access report is created and sent to all managers;

b each manager is required to confirm whether all persons specified as having access to the specific system (for example, EOS) should continue to have access or whether a certain person's access should be removed;

c following that report, any changes to permissions are implemented by the Manage Access and Change Team.

203 However, we were unable to identify with any certainty who has ultimate responsibility for ensuring that this system works as designed. A number of interviewees also identified the risks inherent in a 'human review' process, particularly one only carried out on a quarterly basis, and particularly where there are no clear guidelines or rules for managers to refer to when determining whether access has been appropriately granted. Some interviewees acknowledged the filling out of access reports was deferred and that they knew of cases where staff had moved roles within ACC but their access permissions had not changed as they should. Overall, interviewees had a clear understanding of their own access permissions but found it difficult to explain the overall policy settings and auditing process.

Current approach to permissions

204 As mentioned previously, anyone with access to EOS has open gate access to the entirety of the EOS system, with the exception of sensitive claims, VIP clients, RCU clients, and to staff clients and claims.

205 ACC's policy is to limit EOS access to the files of each client in each of the above categories to a limited number of ACC personnel. No other staff can access these files.

206 So for instance: in the case of sensitive claims, once a claim has a 'sensitive claims indicator' attached to it in EOS, access restrictions are automatically applied. New sensitive claims are allocated within Partnered Recovery through an automatic process (having regard to the capacity of the team members), without the need for others to view the claims. Approximately 865 ACC personnel have access to sensitive claims (as at 18 January 2022). The number of ACC personnel with access has been purposefully reduced since and in response to the publication of the Access Incident.

207 However, there are no limitations on access within EOS beyond the (relatively) discrete categories of 'special' claims or clients. For general claims (that is, not claims by VIP clients, sensitive claims, claims by RCU clients, or staff claims), open gate access automatically applies.

208 In the course of this Review, almost all interviewees were asked directly about ACC's reliance on a high trust open gate setting for information held about the majority of its clients. In particular interviewees were asked why an administrative team member responding to a request to arrange recovery assistance such as signing off access to free taxis (a practice we were told is very common and purely administrative) should also require access to the same client's detailed medical files. In our view, an administrative team member does not require access to medical files to respond to that client's request. As an interviewee suggested:

> You could restrict access for people like payments assessors, people who are doing inbound documents — that kind of stuff. So those people only have access to the parts of EOS they need to see.

209 For context, as at February 2022, of the 2,432 staff with open gate access to EOS:

a 621 staff members provide 'administrative' and 'operational' support (rather than handling claims directly with clients);

b 1,480 ACC personnel work in 'claims handling' (that is, in 'partnered' or 'assisted' recovery roles); and

c 281 ACC personnel work in ACC's northern and southern call centres.

210 ACC's current reliance on open gate access is a policy decision designed to ensure that every frontline worker can answer any question posed by any client contact. In the balance between operational efficiency and privacy protection, this policy tips the scales in favour of operational efficiency.

Access to sensitive claims

211 As mentioned above, ACC limits access to sensitive claims by limiting access permission to a designated group of staff, with each staff member approved by a manager. Nonetheless, Next Generation saw the management of these claims by a discrete unit changed to a distributed model (that is, more eyes potentially accessing each file).

212 ACC has made a policy decision that the information relating to sensitive claims, as well as VIP claims, RCU claims, and staff claims requires more protection than other personal information held by ACC.

213 ACC has recently taken a number of steps in response to negative publicity relating to the Access Incident, as described further in Part 3 (Overview of Snapchat and Access Incidents). These steps involved a significant reduction in the number of staff who can access sensitive claims (reduced from 1,414 staff members to 865 as at 18 January 2022). Other changes include:

a The introduction of a 'sensitive claims' banner in EOS to highlight to any user awareness that the claim is 'sensitive' in nature.

b The introduction of 'capacity streaming' (that is, routing sensitive claims work to a smaller number of staff in each function) across ACC.

c The commencement of work on how user profiles could or should dictate access, that is, by technically restricting which parts of a sensitive claims file can be accessed by particular functions.

d The decoupling of access to sensitive claims from system access lists associated with specific roles and queues. This means access to sensitive claims now requires a standalone request (and justification for access), rather than being packaged up with other systems access requests when someone new begins in a role that may require sensitive claims access.

e The commencement of work to introduce a 'requirement to confirm' banner — that must be acknowledged by staff — whenever a sensitive claims file is accessed.

f The investigation of whether the process for leaders reviewing the quarterly access reports can be strengthened to ensure staff access is routinely removed when no longer required.

214 These changes (not all of which have been fully introduced as of the time of writing) will provide layers of additional protection for clients whose claims are deemed to be sensitive.

215 However, the term 'sensitive' is something of a misnomer. All claims can and do contain sensitive information. As noted earlier in this Review, individuals will have different sensitivities about the information ACC holds about them, but it is uncontroversial to assert that any information about a client's mental health or family living arrangements or income would generally be considered sensitive to them. In fact many clients would regard any information about their health to be sensitive. Yet over and over in this Review, interviewees drew an artificial distinction between sensitive claims and other claims, as if the personal information held in respect of the general claims was in some way less private or able to be managed with fewer protections. Those staff who work with the sensitive claims were particularly activated about the privacy of their clients and subsequently more engaged about ensuring privacy protections are adhered to.

216 Language is important here; signalling to all ACC personnel that all client information is sensitive would send a strong message that all client personal information is precious and subject to the same protections. See our further commentary regarding ACC's approach to privacy awareness and training in Part 8 (Culture).

Challenges with graduated access

217 As noted above, ACC's open gate approach to client information is a policy decision based on the need to manage large numbers of claims efficiently. The majority of ACC personnel interviewed for this Review reported that open gate access was the only feasible approach to client information management, since staff need to be able to quickly locate information so they can more quickly respond to the needs of clients.

218 The impression of this Review is that ACC has a 'zero sum' mindset to open gate access: reducing access is perceived as always creating inefficiencies. Such a mindset is driven by an organisation-wide pressure to meet KPIs and other targets. This pressure is most acute when it comes to call centre staff, where performance is measured against staffs 'adherence' to, among other matters, expected call resolution timeframes. Interviewees reported the view that slower case management is viewed as a hindrance to progression within ACC. In particular, in the case of staff directly engaging with clients (such as call centre staff), a significant number of interviewees considered the unfettered open gate access to general claims (as opposed to sensitive claims, RCU claims, and VIP or staff claims) to be both necessary and appropriate.

219 Equally, many of those interviewed insisted that introducing any limitations on access (for example, of the kind now being contemplated for the management of sensitive claims) for frontline staff was either 'not worth the reward' or simply unworkable, both in terms of quality of service for clients and organisational efficiency. As one interviewee put it, 'holy hell, don't go there'.

220 Introducing limits or electronic gates restricting access to some parts of a client's file would, we were told, simply mean 'more clicks' — more time responding to each request. This was consistently identified by interviewees as compromising efficiencies for the scheme as a whole:

> [...] it sort of becomes a balance of the scheme runs at a level of efficiency and when we tell [the Board] that if we insert another click that actually impacts the time the Claims Manager can get their job done which impacts their KPIs and they are not getting enough claims through a day sort of scenario. I know it sounds pretty harsh that impacts so much so that
>
> they say if you need to put another click in the process then we need another two [full time employees] to be able to fulfil or keep the KPIs up.

221 Another interviewee reflected on the delicate balance between locking down access and service efficiency from a client's perspective:

> At the end of the day, yeah, you can turn around and say I'm going to reduce access right down. Then you are going to make providing the service slower and make it harder and I'm really sure that waiting six months[14] for confirmation that we are going to deal with your broken ankle is not the sort of thing you want.

222 Interestingly, ACC has imposed electronic safeguards to remind staff repeatedly of the dangers associated with sending external emails (a policy response to the 2011 privacy breach). Anyone inside ACC attaching a document to an email is confronted with onscreen reminders asking if they really intend to send the document. This safeguarding procedure creates clicks, yet no interviewee mentioned it as an issue or an impediment to responding to clients in a timely way.

223 Efficiency concerns aside, many of those interviewed expressed the view that the current level of access was a cause for concern, particularly in the context of the very limited monitoring and auditing of access that takes place (which we discuss further below from paragraph 235 below):

> Once you have access to it you can go anywhere in there. We rely on people having signed the Code of Conduct, [and to] know their privacy obligations to not do that [browsing a file] and we can check that footprint now, but we don't have a strong robust process to do that.

224 As mentioned previously, it is clear from the responses that ACC's workforce has been on a dedicated mission to improve efficiency. Daily targets, rewards for resolving client calls quickly and the satisfaction of doing so (given the client demands each day) are strong incentives to resist any change that may — at least at first blush — appear to make the job slower or more cumbersome. Quite reasonably, claims handling staff are resistant to any prospect of having to manage clients whose requests they cannot answer.

225 Customer feedback data, collated by ACC, indicates clients report positively about the improved efficiencies to the claims handling process. But there is a trade-off and we are not convinced that adjusting the balance to give greater weight to privacy protection would generate the issues identified. Certainly no interviewee was able to provide any evidence to support the proposition that, as we were repeatedly told, adding 'one extra click' would require another two employees in each call centre. ACC has confirmed that EOS does have the capacity to provide graduated access levels and improved user profiles. Until now it has been a policy decision not to engage these.

226 Without comfort that information is being protected, the 'quality' of service that comes from a quick response to client queries can only ever be surface level. Building a moat of protection around personal information serves to enhance — rather than detract from — ACC's vision of a quality service for all clients.

Graduated access — a suggested approach

227 At present ACC's starting point is to give all frontline staff open gate access, but then impose limits on access to a smaller subsets of claims. Our view is that this should be inverted; staff should only have access to those tabs or files on EOS where there is an operational necessity for such access, and then

[14] There is no evidence delays of this length would be a consequence of a more graduated access model.

only if that operational basis aligns with the purposes for which the information contained on that tab/file was collected by ACC.

228 The question of access can be solved in a series of principled stages:

a If ACC has a transparent, well defined map of roles with access rights assigned to each then all personnel can identify what access they have and why — this will assist in having them understand their role and the obligations attached to it.

b If the roles are administrative, then access should be limited to information necessary to respond to administrative requests. ACC holds sufficient data to be able to identify with a high degree of accuracy the likely range of administrative issues that will arise in the majority of client calls and align access to those tasks.

c Certain tabs or documents within any file, such as medical files or notes, should be classified as requiring greater protection/privacy and therefore access to these tabs and/or files should be 'gated' with an electronic 'confirm access required' function. Use of this function should be recorded and monitored.

229 We refer to this as a graduated access approach. We are not convinced that introducing a graduated approach to access for general claims will lead to the inefficiencies feared by interviewees. We are also concerned that many interviewees appeared to have reached this conclusion without evidence that the option had been thoroughly investigated. Without robust consideration of the feasibility of introducing graduated access, ACC cannot satisfy itself that concerns of inefficiencies will actually play out as feared.

230 This is particularly the case when it comes to timeliness in providing cover to simple, general claims. For the most part, this category of claim would continue to be automatically serviced through ACC's automated processes, without *any* further need for access by ACC personnel. On that basis, the idea of graduated access leading to a client needing to wait for six months for the outcome of their claim relating to a broken ankle (as referred to by an interviewee, see above at paragraph 221) is not supported by ACC's general approach to claims management.

231 Even starting from ACC's current state view on access (that is, that there is an irrefutable need for all claims handling staff to have access to all client files), according to information provided to us for the purposes of this Review, only approximately 75% of those who currently have access to EOS have an operational need to access all information on a file. The remaining 25% with full, but not justified, access is a not insignificant proportion.

232 As noted at the outset of this Part 7, the systems and processes are simply the tools by which ACC performs its role. As such, those systems and processes should reflect, not lead, the values of the organisation. It is inconsistent for ACC to assert it takes privacy of client information 'very seriously' while at the same time opting for an open gate access policy as the default position.

233 The model proposed here is a lower trust model. This is not to be interpreted as an indication of lack of trust or confidence in ACC personnel. Those we interviewed conducted themselves with honesty and integrity and, largely, with huge attachment to ACC and the work it does. But the organisation's first job is to help its clients recover and rehabilitate after injury and to do that it must retain public trust. Tilting the balance to provide greater privacy protection for clients is an important step to ensuring that the public can provide information without hesitation or concern. In anxious times, that is both a comfort and a necessity.

234 We understand that:

a A current Improvement Initiative is to remediate its database permissions settings, but that such process is intended to take into account the recommendations of this Review. That remediation should take place as a matter of priority for ACC.

b A planned Improvement Initiative for 2022/2023 is to reduce delays in access provisioning across its applications and services and to reduce inconsistent access policies and residual access risk. That exercise should take into account the recommendations of this Review and should be prioritised for completion as soon as practicable (and at least before 2023).

RECOMMENDATIONS: REVIEWING ACCESS PERMISSIONS AND GRADUATED ACCESS

- **R7.3:** Undertake a comprehensive review of the role mapping dictionary that currently exists. An executive team member should lead this, for the purposes of establishing clear guidelines for when any one role will be granted access to EOS, the conditions of that access, and the circumstances in which that access should be reviewed or removed. Such guidelines should be well managed, documented, and understood across all levels of the organisation.
- **R7.4:** Develop and implement a comprehensive and regular permissions review processes, for which an executive team member is responsible, so that ACC can satisfy itself that only those who need to have access to client information actually have access. We would anticipate this process to involve a mixture of automated processes which are supported by ACC's current approach to managers confirming their team member's access, as well as regular accountability checks to ensure those processes are working as intended.
- **R7.5:** Investigate the ways graduated access can be implemented in respect of 'general' claims in a way that does not materially jeopardise ACC's ability to efficiently handle claims. That process should involve at least the following steps:
    - Following the role-mapping exercise recommended at **R7.3** above, ACC should identify the which roles require access to EOS and, with respect to each of those roles, the extent of access required for that role (having regard to the role description and responsibilities). Our suggestion is that ACC start from the assumption that full open gate access is not necessary for the majority of roles.
    - Investigate the introduction of a 'confirm access required' function to appear on screen before any access is permitted to certain types of tabs and/or files. If this function can be added, identify and publish the types of tabs and/or files to be gated in this way. We recommend all medical notes, including notes provided by psychologists, psychiatrists and counsellors be included.
    - ACC should then analyse the actual inefficiencies that are likely to be introduced if graduated access is rolled out (rather than just perceived inefficiencies).
    - Once those inefficiencies have been identified, ACC should consider the materiality of those efficiencies, in the broader context of ACC's statutory functions and its obligations under the Privacy Act.

Monitoring and auditing

235 ACC's reliance on a high trust, open gate model of client information management requires effective and rigorous monitoring and auditing to ensure that management's trust in staff is not being abused and so that, most importantly, clients can be reassured their personal information is being handled with care.

236 The Review identified significant gaps in ACC's monitoring and auditing processes.

237 EOS is configured to automatically record users' access to a claim on a digital footprint. The information recorded on the 'digital footprint' associated with a claim includes:

a the user account that accessed a claim on EOS (which is based on the user's Azure AD profile, and so automatically updates to reflect changes in role as a user moves within the organisation, even in the case of logs for access during the user's previous role).

b the date and time that the user accessed the claim.

238 Each footprint is stored at a database level in an audit table which can be queried by ACC, for instance, in response to a request for information and/or to generate reporting.

239 However, the monitoring processes cannot identify:

a the specific information accessed within a particular claim (that is, which documents and tabs in a client's file were viewed by any one staff member);

b the elapsed time a particular user viewed any one claim; or

c the role of the user at the time they accessed the claim (for example, what prompted the staffer to view the claim — no 'snapshot' of a user's role is taken at the time of access). This would obviously assist in matching access to authorisation.

240 There are no technical or proactive 'triggers' which would automatically alert supervisors or monitors to audit or check access of any file. Accordingly, any review of access occurs reactively, for instance, in the context of an employment problem or following a client complaint.

241 ACC does not conduct regular and proactive spot checks of access. We were told these are commonplace in the two other Government agencies we consulted with and one interviewee reported that ACC had considered introducing them in the past but decided against it. We found this surprising. While ACC has additional monitoring tools (such as call centre analytics software that can be configured to identify trigger words), we were unable to ascertain whether these tools were regularly used to address issues of inappropriate access to client information.

242 Any cross referencing for the digital footprint is an intensive, manual process. While it is possible for ACC to identify whether any one user has accessed a particular claim by pulling the digital footprint relevant to that claim, ACC's ability to investigate the legitimacy of such access is constrained. Undertaking such a review would involve retrieving call logs in respect of the user in question and reviewing those call logs in the context of the footprint. Since ACC's case management approach means multiple persons could technically have legitimately accessed a file, identifying instances of inappropriate access can be extremely difficult.

243 In a related concern, following the Access Incident (referred to in Part 3 (Overview of Access Incident and Snapchat Incident)), the client's advocate identified through her request for a digital footprint of her own file that an ACC investigator who was assigned to look into the client's claim had also accessed the advocate's sensitive claim — twice. ACC's own investigation of this found the access to be reasonable; a decision quashed by the ICRA. The issues raised by the ICRA's finding are beyond the scope of this Review but others interviewed noted that staff were provided with insufficient information about 'what is an appropriate reason to access a claim'.

> When I was in case management, you didn't really think about accessing claims [only] about anything significant. If it was a claim you managed, you could be in and out of it six or seven times a day without thinking about it.

244 Proper monitoring and spot checking would highlight if staff were over-accessing a client's file. However, under current policy settings this kind of review would only be identified after a client's

complaint and even then, for the reasons set out above, coming to a definitive answer about the legitimacy of any recorded access is problematic

245 One issue specifically mentioned in the Terms of Reference is the question of staff browsing in client files, which we address in Part 8 (Culture). While we did not hear or see evidence that browsing occurred, ACC's auditing and monitoring processes are unable to proactively identify browsing or other inappropriate access. As previously mentioned, no spot checks occur.

246 We were surprised to learn of the difficulties that ACC experiences in order to monitor access, particularly since the privacy training received by individuals is predominantly focused on the unauthorised disclosure of personal information (see our further comments in this regard at Part 18 (Culture)). Without a clear roadmap outlining appropriate access and use, as well as clear consequences for inappropriate access and use, ACC is placing significant trust in staff to make the right decisions.

247 While a high trust approach to auditing access to client information may be appropriate for an organisation that deals with a small dataset and enjoys a relatively high level of privacy maturity, this is not the case for ACC.

248 Like many of the other systems discussed in this Part 7, the high trust setting of ACC's limited monitoring and auditing processes is a policy decision. The impression of this Review is that ACC has opted to keep a light touch in respect of monitoring internal use of client information, but a more heavy hand when it comes to the risk of staff sharing information externally. As one interviewee put it:

> The privacy focus has been on the way we manage privacy from an external point of view rather than internal and decisions were made in the early days about how the system we were going to use and what that would enable us to do and so you work to that. Should we have said at some stage we need to think about the [client] information, the access, how will we monitor [access to client information] and all that sort of thing absolutely and that is on us. We didn't do that.

249 We spoke with other Government departments tasked with handling reasonably large datasets, including sensitive information (albeit, not at the volume of ACC). Based on those interviews, our impression is that the auditing tools ACC has in place provide comparatively weaker safeguards than those consistent with best practice. For instance, tools identified by personnel at other Government departments included:

a integrated systems that record all user interactions within a customer database, which enable the Government department to 'replay' the actions of users;

b random monitoring of access to the system (for instance, checking files relating to high profile individuals to check that any access is justifiable);

c quarterly reporting on unauthorised access to a risk and assurance committee; and

d automated alerts for unexpected behaviour or traffic.

250 Interviewees from other Government agencies reported the above tools resulted in a strong call out culture, whereby every person in the organisation could and did distinguish between appropriate and inappropriate use of client information. We discuss further the callout culture at ACC in Part 8 (Culture).

251 ACC's current systems for monitoring and auditing access to and use of client information fall short of best practice. We were concerned to learn from many interviewees that EOS simply does not support the granular and proactive auditing of access.

252 We understand that the Salesforce interface that ACC is in the process of implementing supports the tracking of user actions within Salesforce products (including a user clicking, tapping, or scrolling on a

page) as well as the granular reporting on user 'events'. Interviewees we spoke with confirmed that auditing is not difficult to implement, nor is it difficult to access and query the reporting logs.

253 We have also been told that one of the Improvement Initiatives is to enhance ACC's digital footprint capability to increase the level of detail that ACC can see in relation to which part of a client's claim has been accessed by employees and to support greater oversight of how staff are using their allocated EOS access. However, that workstream is still in an investigation phase only. It needs to be given urgency.

RECOMMENDATIONS: AUDITING AND MONITORING ACCESS

- **R7.6:** Introduce enhanced and regular monitoring and auditing procedures, including 'spot checks', to test access permissions, and to confirm that staff access to and use of client information complies with ACC's privacy obligations (as well as all relevant ACC policies).
- **R7.7:** Appoint a member of the executive team to be responsible for the development and implementation of the regular, randomised, and proactive checks of access described in **R7.6.**
- **R7.8:** Implement a clear policy, for which a member of the executive team is responsible, which establishes the consequences for workers if the above checks reveal inappropriate access to client information.
- **R7.9:** Ensure that the policies and procedures put in place in accordance with **R7.6** and **R7.8** are well understood across ACC (which may include putting in place appropriate mandates and structures to support the implementation of the policy across the organisation).
- **R7.10:** Prioritise the Improvement Initiative to enhance ACC's digital footprint capability with a view to actually implementing (and then using, in accordance with a well-documented and publicised policy) granular auditing tools as soon as practicable.

Systems used by ACC to manage client information

254 The Review is not a technical review of ACC's systems so the following observations are only included out of completeness and because multiple interviewees referred to limitations of the EOS system. While ACC may use other tools to support its provision of services to clients, clients' information is primarily stored on and accessed through EOS.

255 ACC implemented EOS in 2007 (and significantly upgraded the version of EOS used by ACC in March 2019). That being the case, ACC has relied on the tools and functionality offered by EOS for the last 15 years and since then, the scheme moved from a predominantly paper-based to a digitised operation.

256 EOS is an on-premises solution offered by FINEOS Corporation Ltd **(FINEOS),** a company incorporated in Ireland. EOS comprises FINEOS Claim and FINEOS Payments, which together represent the primary claims, client, and payment information system for ACC.

257 While EOS is technically an off-the-shelf solution, it has been heavily configured and customised to suit the business needs of ACC, including by virtue of a number of system updates, patches, and releases over the course of ACC's use of EOS.

258 ACC personnel use EOS for day-to-day operations, including the lodgement of claims, claims assessments, management of claims (including reviews and the management of specific entitlements), and to setup, approve, and process payments and compensation.

259 In terms of user experience, at a high level:

a EOS is essentially divided by claim (rather than by client).

b On an EOS user's dashboard, each claim is divided into tabs which function as 'compartments' for different categories of information. For example, on a claim dashboard payment information is accessible in a separate tab to medical records relating to the client's injury.

c While ACC's expectation is for persons working on a file to only work in the tabs that hold the information they need to access to complete the relevant task, the functionality of EOS does not prevent that person from accessing all information relating to the client (unless the claim is a sensitive claim, RCU claim, or VIP or staff claim, as described above at paragraph 163). We have described this level of access as open gate, since any ACC personnel approved to access the client's file for any reason (for example, to approve and process payments) can also access medical records or other information which we would classify as highly personal.

d While ACC personnel primarily interact with EOS to access records about current claims, EOS is also integrated with other software used by ACC. For instance, through EOS users can access records held on what is called a 'Virtual Client Folder'. This is ACC's repository for case history related documents about a client.

e Other ACC systems also integrate with EOS - for instance, ACC uses Salesforce (a case management application). We were told that increasingly interactions with ACC clients will be managed through Salesforce in future.

f Only ACC personnel can access EOS (and Salesforce). Clients interact with 'MyACC' when providing information to ACC (and that information is ultimately stored on EOS).

260 FINEOS markets FINEOS Claims as 'claims tracking software' that is 'used globally by over 50 insurance organisations'. FINEOS Claims is widely used by large insurance organisations internationally, particularly in the US. However, we were informed only one other New Zealand Government organisations uses EOS operationally, namely Veterans' Affairs New Zealand.

261 Many interviewees identified a number of systems gaps in EOS. Many expressed the view that EOS is better suited as a storage, backend solution rather than a flexible, modern information tool. The impression we were left with was that the system was somewhat inflexible and reliant on information held as PDFs being stored under fixed tabs in each client's file. The majority of client information that ACC receives is provided through PDF.

262 One interviewee summarised EOS as 'ultimately [...] a repository, it's a database you know'. Another said:

> Our systems do not support us in the way that they should do, which is incredible when you think about the scale and resources of this organisation.

263 The Terms of Reference of this Review do not extend to a technical review of the information systems ACC relies on. In any case, some of the frustrations expressed about EOS as the backbone system for information collection, storage and use may, in fact, be more about how the system is configured, than about the system itself. That said, overall, our impression is that the functionality offered by EOS is not in itself an impediment to high quality protection of client information, provided the proper protections and controls are in place.

264 As part of a systems development project following the implementation of Next Generation (see our commentary from paragraph 176 above), ACC is currently in the process of implementing a new interface for a number of its systems, including EOS. That interface (offered by Salesforce) will provide a layer over top of EOS with which users will interact. While the functionality of that interface is still under development, one aim of this project is to provide ACC with better visibility of clients within its system so as to make it easier for ACC to assist clients in their recovery. However, we understand that the current approach to permissions, access, monitoring, and auditing the use of ACC's client information systems will not change with the introduction of this new interface.

265 The introduction of a new interface (albeit, one still reliant on existing systems) presents a unique opportunity for ACC to identify, implement, and deploy safeguards to better protect client personal information. ACC should use this opportunity to strike a new and improved balance between operational efficiency and privacy protection.

Part 8
Culture

8 Culture

266 This Part 8 discusses ACC's overall privacy culture, the cultural shift that occurred in 2012 following the 2011 privacy breach, and the culture gaps that still exist and which form the background to the Snapchat Incident (and to a lesser extent, the Access Incident).

267 In short, this Part 8 concludes the following:

a **ACC's overall privacy culture:** ACC has expended significant time and resource to remedy the issues that led to the 2011 privacy breach (discussed in greater detail at paragraph 278 below). However, this has resulted in a reactive, rather than proactive, privacy culture that is driven by a fear of breaches occurring and, more particularly, one kind of breach occurring. ACC's privacy culture is narrowly focused on avoiding a repeat of what occurred in 2011 — manual handling or human error. This has two consequences: first, ACC's culture lacks the maturity to ensure that personal information is a taonga to be protected; and second, without that values based approach privacy is treated as an operational issue rather than the cornerstone of an information based social contract. See our further comments at paragraphs 268 to 276 below.

b **A cultural shift occurred in 2012:** ACC's privacy culture is very much shaped and founded upon its response to the 2011 incident and 2012 Independent Review. Now is an opportune time for another cultural shift to further cement and enhance the work ACC has done since 2012. See our further comments at paragraphs 277 to 305.

c **ACC's privacy culture needs to be values based and more mature:** ACC's focus on human error breaches indicates the need for a more rounded and mature privacy culture. ACC's operational approach to privacy has encouraged staff to develop privacy 'blind spots' or silos. Addressing these will help prevent incidents such as the Snapchat Incident occurring again. See further our comments at paragraphs 306 to 337

d **ACC should address other cultural factors:** Addressing factors such as staff training, ACC's callout culture and working from home environments may also have provided protection from further privacy breaches. See our further comments at paragraphs 338 to 411.

General privacy culture

268 As already noted in Part 1 (Introduction), ACC holds an incredibly large volume of personal information. This information is the core ingredient that allows ACC to perform its functions. Equally, it is essential that any injured New Zealanders can and do trust ACC, since ACC cannot provide recovery, rehabilitation support or compensation unless the injured agree to share their personal information.

269 The vast majority of information collected by ACC (beyond basic contact information) can be characterised as the most sensitive types of personal information — an individual's health information. This information varies in sensitivity from basic information contained in an ACC45 form about an ankle sprain received while gardening, to detailed medical reports about traumatic and serious injuries, mental health information and information about sexual assault and on-going trauma.

270 Many persons interviewed for this Review clearly felt strongly about privacy — their concerns about the potential consequences of particularly the Snapchat Incident on the public's trust in ACC were genuine and commendable. But this Review identified a disconnect between the sentiments of some of those interviewed and the overall privacy maturity ACC experiences as an organisation. This is not a reflection on the individuals concerned, but the organisation generally. Addressing this requires much more than a series of `technical fixes'; it requires a cultural reset.

271 The documents we reviewed and the interviews we conducted with a range of staff from different parts of the organisation demonstrated that ACC's privacy culture is driven principally by reactiveness and in particular by the fear of privacy breaches, rather than any positive affirmation of privacy protection as a core value. That said, we acknowledge at the outset that ACC says of itself that it `takes the privacy of client information very seriously'.

272 Among the interviewees, very few of the staff were able to provide an accurate definition of what constitutes a privacy breach. When asked what a privacy breach was, most gave the same or similar example of an inadvertent breach — for example, sending medical documents to the wrong provider. There seemed to be very little understanding that other behaviours can also be a breach of privacy, including sharing information about a client to team members who have no reason (that is, authority) to have access to that information.

273 We gleaned a strong impression about the culture from a variety of sources, almost all of whom were consistent:

a ACC has a stringent process in place to avoid staff inadvertently sending client information to the wrong person by email. Universally, staff understood this conduct to be a breach of privacy. It was evident that staff are strongly motivated to avoid a repeat of the breach that occurred in 2011. However, the focus on this event and this type of breach appears to have inadvertently encouraged a somewhat narrow understanding of what constitutes a breach. This in turn has influenced wider workplace attitudes to privacy protection.

b Contact centre staff members talked about routinely conducting a `privacy check' with clients, by which they meant ensuring that they are talking to the right person before fully engaging with a client on the call. It appears, for some staff, once this `privacy check' was complete, privacy was no longer a concern. One contact centre staff member we interviewed said `that was my greatest fear... that stuck with me, you just always have to get the privacy check right'.

c When asked how success in privacy was measured, staff in the privacy team pointed to the number of privacy breaches; identifying trends in reporting over time. This is reflected in other reporting and documents provided to the Review. For example, in a 2016-2020 Privacy Maturity Plan, when assessing progress since the 2012 Independent Review conducted by KPMG (into the 2011 breach), ACC talks about improvements that have been made, but notes `...privacy breaches are still occurring. Our processes are still manually intensive and rely on the attention of individual staff members to avoid mistakes being made'. Similarly, an executive staff member interviewed for this Review referred to monthly reporting of privacy breaches as an example of how success is measured.

d Other tools identified by the privacy team as being in place to build a privacy culture, such as privacy training (which we discuss in more detail below, at paragraphs 354 to 366) and monthly newsletters, also focus on privacy breaches. For example, the privacy newsletters single out successes in avoiding `near misses' and these were, in the examples we reviewed, almost always near misses of the type of breach discussed above.

e ACC's `Privacy Assurance Framework' (undated) lists ACC's five lines of assurance for privacy. The document focusses overwhelmingly on risks and risk management — the first line of assurance is `recognise risks and proactively manage their risks' and the final line is `overall responsibility [for] ensuring risk management in place'. None of the assurance lines refer to a broader privacy culture or reflect an understanding by ACC that building a strong, positive privacy culture is one way to manage privacy risks, and perhaps the most long lasting and effective.

f ACC's 2020 Government Chief Privacy Officer Annual Agency Self-Assessment Report notes 'the reporting of near misses has remained consistent, which is reflective of our strong privacy culture'. This reflects an understanding that recording breaches equates to success or failure for

privacy performance and privacy culture. Again, this examines the issue of privacy protection through a reactive lens. The focus is on not repeating the mistakes of 2011, rather than building a privacy culture through positive, values-based engagement, expectation and repetition.

274 During this Review, we were consistently told that ACC took privacy seriously and that the organisation was committed to a strong privacy culture. ACC's own impression is that it manages privacy well. By way of a few examples:

a As noted above, ACC's own privacy self-assessment refers to reporting of near misses as being 'reflective of a strong privacy culture'.

b ACC's Privacy Compliance Dashboard (undated) refers to the fact that:

> 33 per cent of NZers surveyed as part of Colmar Brunton's 2018 RepZ survey agreed that ACC can be relied upon to protect individuals' personal information. This is a 2 per cent improvement from 2017 and 1 per cent higher than the Public Sector average

c ACC's 2016-2020 Privacy Maturity Plan states that since the 2012 Independent Review:

> we have made significant improvements and investment in our privacy performance... including the establishment of a dedicated privacy team, and client information teams to manage information access requests.

275 Our impression, however, is that the reactive focus on avoiding breaches means that ACC's privacy culture, while strong in some senses (its efforts to minimise and report breaches, and train staff to avoid them), is weak in others.

276 The culture is not one that helps staff, particularly new and younger staff, to understand:

a the large volumes of information that ACC holds;

b the incredibly sensitive nature of the information (relating to all clients and not just those assigned to sensitive claims);

c the fact that everyone at ACC has a role in protecting personal information;

d ACC's obligations under the I PPs to ensure personal information is appropriately collected, used, and stored; and

e the wide variety of ways that privacy can be breached, including by unauthorised or unnecessary access or internal use of personal information. Further, from the point of view of operational staff at ACC it is not clear that, beyond avoiding and measuring privacy breaches (as described above), protection of personal information is an organisational priority and/or who in the organisation takes the lead in privacy.

Cultural shift following 2012 Independent Review

277 It was apparent from a range of interviewees that following the 2012 Independent Review the organisation underwent a deliberate and purposeful cultural shift. The 2012 Independent Review was commissioned by the OPC and the ACC Board after a significant data breach on 5 August 2011.

Summary of the 2012 Independent Review

278 The 2011 breach involved the unauthorised disclosure of the details of 6,748 ACC clients. A spreadsheet containing details of clients' reviews with Dispute Resolution Services Limited was sent in error in an attachment to an email to a client. Dispute Resolution Services Limited managed facilitation, mediation, and review hearings for ACC clients who were unhappy with a decision or outcome related to their claim.

279 ACC was not aware of the breach until around four months after it occurred. Once aware of the breach, ACC asked the client to return the information, however the full seriousness of the breach only became apparent when details of the incident were released to the media in March 2012.

280 The terms of reference of the 2012 Independent Review required KPMG to assess:

a the circumstances of the breach, including the cause(s) and ACC's response;

b 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);

c 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; and

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

Findings of the 2012 Independent Review

281 The 2012 Independent Review found that ACC should have done more to follow through on the breach once it was notified that client information had been shared, and escalated the issues to the Privacy Officer and/or the Office of the Complaints Investigator. ACC should also have done more to ensure the information was returned and should have conducted a more extensive internal investigation into how the information was sent to the client in the first place.

282 While the breach was a genuine error, the 2012 Independent Review identified systemic weaknesses in ACC's culture, systems, and processes. It identified the use of dual monitor screens, extensive use of spreadsheets for management reporting, a variable culture in respect of the importance of dealing carefully with personal information, and lack of clear accountability for addressing privacy issues as key issues which led to the breach.

283 In addition, there was not a clear culture of privacy being everyone's responsibility. Some work practices (such as physical file copying and distributing physical files in response to access requests) and system design (such as open access to most client data once someone has access to the claims management system) could result in inappropriate disclosure of personal information when not reinforced by a culture where the importance of personal information is understood.

284 The 2012 Independent Review found that ACC's risk management framework was lacking, as it did not include risks associated with collecting and managing personal information as a core part of the framework. Privacy management was more focused on responding to the breaches than actively managing personal information in line with the IPPs.

285 The Privacy Officer did not act as a central coordination point for all privacy matters across ACC, they simply dealt with escalated issues. There was no comprehensive privacy programme and

accountability was not clear (including for escalating and resolving issues). As a result, monitoring and reporting of privacy matters was limited.

286 The 2012 Independent Review concluded that a similar incident was likely to happen again if the identified issues were not addressed systematically and systemically.

Recommendations of the 2012 Independent Review

287 The 2012 Independent Review was a comprehensive exercise, resulting in 44 recommendations across seven categories:

a Board governance.

b Leadership and privacy strategy.

c Privacy programme.

d Culture.

e Accountability.

f Business processes and systems.

g Backlogs and establishment of the new Business as Usual.

288 The 2012 Independent Review stressed the importance of creating a culture of respect for client privacy and good management of client information, and made a number of recommendations relating to this. For example, it recommended adopting a privacy strategy covering the values and principles necessary to develop a culture which supports the privacy strategy. The privacy strategy should state the importance of a culture of respect for client privacy and good management of information about clients. It also recommended creating a culture in which everyone has ownership and responsibility for protecting personal information through strengthening the 'three lines of defence model'.

289 However, while the 2012 Independent Review recognised the importance of understanding the I PPs and a culture of privacy awareness, many of the recommendations related to risk management,

reporting, preventing data breaches, creating accountability roles, and auditing. For example:

a Under the 'Board governance' recommendations, the 2012 Independent Review recommended ensuring that there is continuous accountability to the Board by leadership for privacy risks, and recognising that 'zero acceptance' of data breaches requires minimising risks at all stages of the information management life cycle.

b Under the 'Leadership and privacy strategy' recommendations, the 2012 Independent Review recommended that a privacy strategy be adopted which implements a clear structure of responsibility and accountability for implementing privacy compliance and best practice, as well as mechanisms for ensuring best practice and compliance is integrated into new systems, products, and services.

c Under the 'Privacy programme' recommendations, the 2012 Independent Review recommended that the role of the Privacy Officer include providing advice on privacy by design principles. The Privacy Officer should also implement training that is operational, scenario-based and practical. These recommendations also include suggestions that processes be implemented to manage near misses, privacy breaches, and complaints.

d Under the 'Culture' recommendations, the 2012 Independent Review recommended that staff be encouraged to report and resolve breaches, and develop measures to test respect for client privacy.

e Under the 'Accountability' recommendations, the 2012 Independent Review recommended that KPIs be implemented to assess privacy management performance and that performance against these are monitored.

f Under the 'Business processes and systems' recommendations, the 2012 Independent Review recommended that ACC review the claims management process with a particular focus on:

i ensuring compliance with ACC's obligations under privacy laws;

ii ensuring process controls are effective;

iii identifying high risk processes;

iv implementing an 'enter once' policy for data entry and reporting systems; and

v automating KPI and reporting processes.

After undertaking this review, ACC should look to re-engineer processes to adopt a privacy by design approach in order to minimise risks.

g Under the 'Backlogs and establishing of the new Business as Usual' recommendations, the 2012 Independent Review recommended that ACC add additional resources to clear backlogs related to privacy issues.

Independent Privacy Follow-Up Review (2014)

290 In 2014, KMPG undertook an Independent Privacy Follow-Up Review (Follow-Up Review). It assessed ACC's progress towards implementing the recommendations made by the 2012 Independent Review.

291 It found that since the 2012 Independent Review, ACC had focused mainly on changing how it dealt with clients' personal information and how that information was viewed by staff. The Follow-Up Review identified a cultural shift towards continual improvement of privacy processes amongst frontline staff. However, there was also frustration with KPIs. Some KPIs focused on the volume of claims dealt with in a day and others focused more on quality (for example, careful privacy checks).

292 The Follow-Up Review found that systems and processes were largely the same, albeit with increased detective controls to identify issues. Many of the controls were manual and reliant on individuals to follow appropriate processes so human error remained an ongoing cause of privacy risks.

293 Overall, while good progress had been made, the risk of a future major privacy breach was still relatively high (albeit reduced since the 2012 Independent Review).

294 The Follow-Up Review made further recommendations, which also tended to focus on formal risk management measures and processes. For example, it recommended further development of measures based on privacy by design, and:

a Reviewing and enhancing the Privacy Strategy by developing a privacy performance measurement framework (including relevant KPIs) which should be based on specified requirements that cover all aspects of the 12 I PPs contained in the Privacy Act. The definitions of breaches and near misses should also be reviewed.

b Resolving the perceived discrepancy between quantity and quality KPIs for staff.

c Enhancing the enterprise-wide three lines of defence operating model to enable better integration with privacy risks, and compliance and assurance frameworks.

Cultural shift following 2012 Independent Review

295 It was evident from many interviews that the events of 2011 and 2012 were scarring for ACC staff and the organisation itself. There was, in the wake of the 2012 Independent Review, a strong commitment led by the Board and senior executives to do better in future. It continues to be a predominant focus of the privacy team and privacy strategy. For example, in its September 2020 privacy newsletter ACC notes -

296 ACC is very, very sensitive about privacy breaches: the 2012 incident where thousands of claim numbers and names were accidentally emailed to a client still looms large in our corporate memory.

297 Since then ACC has implemented many of the recommendations in the 2012 Independent Review and key recommendations — the role of the Privacy Officer, the focus on avoiding future breaches and developing a privacy by design approach — remain key planks of ACC's privacy management in 2022.

298 However some significant recommendations have still not been addressed. For example, the 2012 Independent Review urged ACC to take steps to create a culture of respect for client privacy under which everyone in the organisation has ownership and responsibility for protecting personal information. We did not find evidence of this; a mature understanding of privacy is not embedded in the organisation (although a narrow interpretation of privacy is).

299 Likewise, the 2012 Independent Review's caution about the reliance on physical file copying and 'open access to most client data' appears to have been side-lined (as discussed in Part 7 (Systems)).

300 The 2012 Independent Review recommendation that ACC strengthen its three lines of defence model for privacy included a recommendation that ACC ensure a member of the executive is accountable for privacy and is responsible for providing leadership on the implementation of ACC's privacy strategy. As we will explain in greater detail at paragraph 323 below, there remains no single member of the executive who is ultimately accountable for privacy or responsible for providing privacy leadership. Instead responsibility is divided at different levels of management, according to operational tasks.

301 We were unable to find out why this might be the preferred approach. Questions seeking a definitive answer about why certain practices were or were not adopted tended to turn into a frustrating information trail, with one interviewee after another referring the question to a colleague 'who will know'. We did not interpret this to be a deliberate obfuscation. Without exception interviewees cooperated willingly and with candour. However, with responsibility distributed across different roles, accountability for privacy is opaque and answers are hard to find.

302 One potential consequence of this is a vacuum of leadership which, in our view, could explain why —despite the best of intentions - ACC's response to the 2012 Independent Review has been concentrated on operational matters, rather than addressing wider and underlying cultural issues. This is an opportunity lost.

303 In this context, ACC's policies, training, corporate documents and overall culture are guided by reactiveness — primarily focused on preventing the type of breach that gave rise to the 2012 Independent Review (preventing information from being sent to the wrong person). Managed in operational silos, policies and initiatives have been principally aimed at procedure and processes, rather than developing a privacy-centric values based culture as recommended by the 2012 Independent Review.

304 As discussed below at paragraph 353, this Review acknowledges that ACC has undertaken significant work and invested significant resources to remedy the problem that led to the 2011 incident. It is also clear that ACC's privacy understanding and knowledge has grown significantly since 2012; there has been a cultural shift. By way of perspective, until the Snapchat Incident, ACC had not experienced a major privacy breach since 2011. Given the amount of information held by the organisation and the number of daily interactions staff have with clients and third parties that reflects well on ACC and its staff.

305 However, the issues arising from the Access and Snapchat Incidents that concern this Review, provide an opportunity for further improvement so that, as the 2012 Independent Review originally envisaged, protection of personal information is at the forefront of every ACC worker's mind and all staff understand that protecting personal information goes much further than ensuring the right attachment is sent to the right person in an email.

How improving ACC's privacy culture may prevent further incidents

306 The Terms of Reference require this Review to consider the issues arising from the Access Incident and the Snapchat Incident.

307 In terms of the organisation's culture those issues which can be identified in respect of the Access Incident are:

a ACC's high trust open gate approach to client personal information, which results in many eyes potentially accessing one file;

b the general expectation among frontline staff that they must or should have open gate access and the impact this has on how they think about and value personal information;

c the disconnect between staff expectations and client expectations, who may believe access to their personal information is more tightly protected; and

d the difficulties the organisation has in actively monitoring and auditing staff usage, which are well known to staff at all levels.

308 These are issues largely addressed in Part 7 (Systems). We do not consider that there are widespread cultural factors that contributed to this incident. Rather, we think there are structural or systems factors that contribute to many eyes viewing a client's file and the fact that, on learning how many people viewed the file, clients may be quite reasonably concerned and/or distressed.

309 That said, addressing the cultural factors identified in this Part of the report could in fact reduce the number of staff accessing any particular file since embedding a mature values-based privacy culture should encourage staff to think more carefully before they access any file, or any part of a file. Do I have a proper purpose for looking at this file? Or, do I need to look at this information to respond to this request?

310 In respect of clients' expectations, in Part 7 (Systems) as part of our recommendation that ACC introduce a roadmap of client information, we recommend that a customer facing version of this roadmap be developed so that all clients understand why so many people may need to view their file (see **R7.1** and **R7.2).** ACC should ensure that it can, from a systems perspective, provide detail to clients about what parts of their file have been viewed and why. We would expect clients to be less concerned or distressed by digital footprints showing access to their information by ACC staff if those clients are also provided with information about how many accesses involved a review of their medical information versus how many just involved access to accounting or other basic information.

311 In terms of the organisation's culture those issues can be identified in respect of the Snapchat Incident are:

a trust and respect, or the lack thereof;

b the apparent lack of a values based understanding of the importance privacy plays in what ACC does and how clients interact with the organisation;

c the narrow definition of what constitutes a privacy breach;

d the way ACC inducts and trains staff and later reinforces that training;

e the increase in ACC personnel working from home and in isolation from other staff and the potential impact this has on staff welfare and communication;

f ACC's call out culture; and

g the use of social media as a regular communication tool between personnel.

312 These issues are addressed in this Part 8. While these issues were identified by the Review as being a factor in incidents such as the Snapchat Incident, many were also identified by staff during interviews.

313 The Review also identified additional cultural issues which impact ACC's compliance with its privacy obligations:

a the cultural implications of the introduction of Next Generation;

b the language used by ACC — 'claims' versus 'clients' and the use of 'sensitive claims'; and

c a high degree of turnover amongst ACC staff.

Trust and respect, or the lack thereof

314 What happened on Snapchat demonstrated a fundamental lack of respect for client personal information. Without exception, staff interviewed for this Review all understood this and expressed shock and distress at what had occurred. Publicly posting or sharing any information gleaned from a client's file is never acceptable and in the case of the information posted on Snapchat it was evident that those concerned were using the information as entertainment or amusement. This was and always would be a serious breach of trust and privacy.

315 The fact that, for whatever reason, some ACC workers chose to do so demonstrates that ACC's pledge that it 'takes the privacy of client information seriously' is neither universally understood nor applied.

316 We heard no evidence that other staff had or were posting similar material on social media, although other staff confirmed they too were members of social media chat groups with other ACC workers (past and present) and that these or similar informal chat channels are not uncommon.

317 The significant feature of the Snapchat Incident group was the posting of screenshots from client files and, further exacerbating the breach, the tone applied to that information. This conduct showed a complete lack of respect for clients and their privacy rights. Those ACC personnel working with victims of sexual assault were particularly concerned about the impact the incidents may have on public trust in ACC, fearing publicity about the Snapchat Incident would potentially deter some victims from coming forward to seek assistance from ACC.

Lack of a values based understanding of the importance privacy plays in what ACC does

318 Interviews with staff and a review of key documents evidence a lack of a values based understanding of the importance privacy plays in what ACC does. While privacy is taken very seriously, this comes from fear of another breach occurring rather than a values based sense of kaitiakitanga to protect the taonga that is personal information.

319 This lack of a values based approach arises for a variety of reasons — the way ACC responded to the 2011 breach and subsequent 2012 Independent Review (discussed above), together with continuous change within the organisation — including both its systems and its personnel, and potential shortfalls with the current organisational structure (discussed further below at paragraphs 320 to 337).[15]

RECOMMENDATION: CULTURE GAPS

R8.1: Conduct a comprehensive review of the various tools, systems, documents and guidance ACC currently uses to shape its privacy culture and consider how these can be modified to ensure that all staff are taught that key privacy values, such as the fact that privacy is important and that it should be protected at all costs.

This review should include, at the least, the following:

- Consideration as to whether the current tools such as privacy newsletters or the use of the privacy team to answer questions, are effective at delivering broader cultural messages. Assess what other options, such as a values statement or other guiding principle, may assist to develop this privacy culture.
- The introduction of measures and targets to gauge the strength of its privacy culture and performance that go beyond breach reporting. For example, ACC could implement measures and/or targets in respect of the completion rates of privacy training, number of visits to the privacy intranet page, and staff surveys on awareness and understanding of privacy values. ACC could also measure and assess the questions the privacy team receive from staff to identify gaps in understanding and put in place refresher training or further guidance to plug these gaps.

We understand that ACC's Improvement Initiatives include various pieces of work to improve its overall privacy culture, including an external review of Privacy Maturity, independent legal feedback on its privacy documents, a refresh of frontline engagement and knowledge collaboration, and benchmarking against other agencies. We strongly recommend that ACC undergo these initiatives with the fundamental culture change recommended above as a starting point, to ensure that the initiatives do not serve to perpetuate the status quo — the focus on breaches.

Role of the privacy team and organisational structure

320 Embedding privacy protection into the culture of an organisation requires roles and responsibilities committed to privacy at all levels of the organisation. The Review identified a real gap in ACC's privacy organisational framework, despite the organisation having a Head of Privacy, a Privacy Officer and a sizeable privacy team, albeit in an organisation of over 4,000 people.

321 ACC's privacy team was created in response to the 2012 Independent Review. At full strength, ACC's privacy team comprises 12 people, including:

a a Head of Privacy (the team's manager);

b a Privacy Officer;

c two senior advisors and four advisors;

d a business reporting analytics advisor; and

e a research advisor — ethics.

[15] During the period of this Review, ACC commenced a review of its organisational structure. We have not been provided with information about this we make no comment on whether the proposed changes will address the issues identified in this report

322 In reality, churn and a number of vacant positions means that ACC has not experienced a consistent and fully staffed privacy team over the last few years. At the time of writing the team has a number of vacancies.

323 The Head of Privacy reports to the General Counsel, who is a member of the Executive. Neither the Head of Privacy nor the General Counsel have full oversight of all aspects of privacy and it appears no person in the Executive team has ultimate responsibility for privacy (despite this being recommended by the 2012 Independent Review). No single member of the executive was identified as having overall responsibility or oversight for EOS generally, which is also of concern given EOS is the repository for the majority of client information at ACC. This again reflects the silo approach adopted by previous ACC senior managers in response to the 2012 Independent Review.

324 We see this as having two potential implications:

a Other than weekly reporting on breaches to the Board (and monthly to the Operations team), there was no sense that the Executive team had oversight or accountability for how the organisation was performing from a privacy sense. As discussed above, breach numbers are not the only success (or failure) measure for privacy.

b Without full executive team leadership it is difficult to nurture an organisation wide understanding and respect for privacy protection. Values driven change requires champions with authority to ensure that the necessary changes are prioritised and implemented.

325 When we spoke with staff from the privacy team, they reported that the majority of their time was spent handling privacy breaches, dealing with queries from the organisation or preparing PIAs or Privacy and Ethics Threshold Analyses (**PETAs**). This represents a high volume of work. According to ACC's Improvement Initiatives, as at February 2022, the privacy team was working on over 70 privacy assessments. This is a significant workload.

326 When asked how the privacy team builds privacy culture and privacy values within ACC, we were pointed to the monthly newsletters the privacy team sends out and the role they play answering queries from the business. We were also advised that, prior to COVID-19 related restrictions, the privacy team would visit the regions to make themselves visible, provide training (although no details about what that training entailed were provided) and answer queries in person. These are all positive initiatives, but either individually or together, they have not to date succeeded in embedding a mature understanding and respect for protecting client information.

327 The lack of representation at executive level, and the privacy team's own description of how its hours are spent, goes some way to explaining why staff throughout the organisation described the privacy team as 'advisors' who lack 'clout' or power to bring about change. One person noted the privacy team was a 'go to' team when something has gone wrong or someone is worried'. A number of interviewees reported that they would always call the privacy team if they had a question and that the team were approachable and helpful.

328 The privacy team has an important role to play in building up the organisation's privacy values and culture. They can play a key role in driving the necessary cultural shift. But the fact others in the organisation perceive them to be advisors only (and they act as advisors) limits their effectiveness as leaders of cultural change.

329 ACC's siloed organisational structure is another factor hampering the privacy team's effectiveness. To give just one example; a complaint about a potential privacy breach resulting in an investigation in to the conduct of an employee has usually been managed as an employment matter, not a privacy is sue and, accordingly, the privacy team may have no visibility of what happened or why. Consideration will need to be given to how the workloads of the privacy team are managed so as to enable appropriate capacity and capability. ACC should also consider the team's mandate so as to better ensure cultural change.

330 The need for an objective external review of Privacy Maturity was raised in June 2021 by the incoming Executive team, to be led by the then-yet appointed Head of Privacy. A permanent appointment to that role was made in September 2021. On 30 September 2021 the Board was asked to consider whether such a review should proceed. The Access Incident occurred several weeks later, and this Review was commissioned. We recommend that the recommendations of this Review should be prioritised for completion as soon as practicable and progress reports incorporated into future reports to the Board, OPC and / or ACC's external monitor.

RECOMMENDATION: ROLE OF PRIVACY TEAM

R8.2: Implement changes to the organisational structure, capability, and mandate of the privacy team (including the Privacy Officer role) to ensure:

- that the privacy team has sufficient influence to bring about change where required. This should include a consideration of whether any changes are required to role descriptions, resourcing or the privacy team's day-to-day tasks to allow them to spend more time building (and measuring) ACC's privacy culture and working to build a set of privacy values;
- that a member of the executive has overall accountability and responsibility for privacy;
- that measures are put in place to support enterprise wide execution and support of changes recommended by the privacy team; and
- that the executive leadership team has sufficient oversight of all privacy matters (including those that go beyond reporting on breaches).

Drive for continuous change in ACC's systems

331 Many staff talked with pride about privacy by design, agile release trains and continuous improvement.

332 As we understand it:

a Privacy by design is a model whereby any new system or any change to a system is considered through a privacy lens prior to implementation. During interviews and in our review of documents, we were unable to ascertain precisely what privacy by design means in the context of ACC (even though a number of interviewees referenced it) or how it is undertaken. The focus is generally on the completion of a PIA or PETA.

b Agile Release Trains (ARTs) are a model of continuous improvement whereby continuous small changes to systems are made as issues are identified. One interviewee described it as 'all about the business coming up, making change and getting it back into the business to add value, increase efficiencies and all that sort of stuff'.

333 Interviewees reported that ACC is continually working on a number of small projects to improve. We were told this had been a strong focus over the past six years. One staff member noted:

> we are very reactionary... it's almost like we are playing...whack-a-mole, where something pops up, we get the low hanging fruit and we knock it back down again, but we don't think about the bigger picture.

334 Not thinking about the bigger picture is one explanation for why, having exerted so much effort and resources to responding to the 2011 privacy breach, the organisation has still failed to embed an underlying positive privacy culture and why privacy continues to be viewed through a narrow lens. The reliance on privacy by design, for example, is only triggered by some new initiative being in train. A proactive approach may have identified, for instance, that having contact centre workers working at home and in isolation from one another (as happened as a result of COVID-19) had privacy implications. In fact, no privacy analysis took place before or after workers were sent home to work.

335 In addition, some interviewees expressed concern about the effectiveness of PIAs or PETAs. A handful of staff gave an example where incorrect information had been given during the PETA process. This resulted in the finding of the PETA — that the change or system it was assessing had no or a low privacy risk — being false. In turn, this led to personal information being shared when it shouldn't have been shared. The carrying out of PETA and PIAs once a new system has already been put in motion risks identified privacy issues being dismissed out of a desire to quickly and efficiently introduce the system. We have recommended that PETA and PIAs are completed before a new system is put in motion, to help to ensure that privacy values are embedded at the very start, rather than being shoehorned into a process that is already underway.

336 Other staff we interviewed expressed concern about the fact that PIAs and PETAs are signed out by the project managers and the Privacy Officer, which may result in them having less 'clout' or weight within the organisation. Some staff commented that this level of signout made it difficult to address the issues that arose in the example noted above. ACC has advised that internal work is underway to assess the effectiveness and efficiency of these processes.

337 One of ACC's Improvement Initiatives for April/May 2022 includes the organisation seeking assurances on 'effectiveness including whether the information collected through PETA accurately reflects the information management and privacy risks of projects, to inform resource allocation and around follow up and implementation of PETA recommendations by project teams'. We consider that changes are required beyond the seeking of assurances, and recommend that ACC implement the above changes as a priority.

RECOMMENDATIONS: PRIVACY ASSESMENT PROCESS

- **R8.3:** Consider how to ensure that PETA and PIA assessments are not a 'box ticking' exercise. As part of this ACC should consider how to ensure that privacy assessments are done *before* a new system or model is put into motion, rather than after.
- **R8.4:** Asses what changes are required to ensure that PETAs and PIAs are afforded sufficient weight within the organisation. This should include:
    - requiring PETAs and PIAs to be signed out by the Head of Privacy to ensure that the assessments are given a greater degree of importance throughout the organisation; and
    - requiring the Head of Privacy to provide quarterly reports to a member of the executive about the number of assessments and the recommendations made.
- **R8.5:** Review the thresholds for when privacy assessments are required. This should include:
    - ensuring that PIAs and PETAs are completed that when there are major changes to systems or work practices (such as a move to working from home) rather than only when new systems are introduced; and
    - considering whether a PETA/PIA (or full PETA/PIA) is required for every systems change.

Narrow definition or understanding of 'privacy breach'

338 As discussed above at paragraphs 268 to 276, the Review highlighted that ACC's privacy culture is typified by:

a a focus on privacy breaches as the sole (or major) indicator of success or failure in privacy; and

b a narrow definition or understanding of what a privacy breach is.

339 In our view, as further demonstrated below, the narrow understanding of breach is a risk factor indicating other incidents could occur because:

a If staff do not fully understand all of the behaviours that constitute a breach, ACC cannot be confident other breaches won't occur.

b ACC's culture, training, policies and systems do not appear to teach staff that internal misuse of a customer's information is a breach of privacy.

Sharing on social media

340 The Snapchat Group appeared to be under the (mistaken) impression that because they were sharing information between ACC staff this was not a breach of privacy. This demonstrates a fundamental lack of understanding of the fact that use of the information must be connected to the reason it was collected in the first place.

341 While we found no examples of other staff posting client information on social media, we were told that staff discuss cases involving clients with each other 'from time to time'. Some of this conversation will be lawful because it will be one staff member seeking assistance or review in the interests of assisting that client. But other interviewees admitted that after difficult calls call centre staff need to 'debrief' to release stress. It is likely in these exchanges client information is, or may be shared, without proper authority. We identified no specific training or guidance on this point. By contrast, a privacy officer from another Government agencies told us that staff at that agency were specifically cautioned about these kinds of conversations and, if they occurred, staff would report it

so that further training could be provided. The apparent lack of similar protections at ACC reflects the way privacy is defined, which leaves too much room for misunderstanding and mistake.

Browsing of client files

342 We asked staff about the prevalence, if any, of staff browsing client files.

343 One interviewee said 'it was made very clear... you don't go searching for your own personal information. You don't go searching up your family members or friends'. While correct, it is not clear where this staff member received this instruction. None of the documents, training, policies or other items we reviewed made staff aware that browsing of this nature is not allowed. In the absence of written material, it is likely then that staff are provided with inconsistent training or guidance on this issue. In fact, one interviewee signed in and attempted to view their own profile during the interview (this unsuccessful attempt was to make a point about the lack of controls on access, although the interviewee noted that the system appeared to have tightened since they last accessed their file).

344 Another staff member commented that 'it was never something that was on my radar that I should be ensuring I only access a claim if I have a strict purpose' (they gave the example of opening a claim multiple times because they had been distracted and not completed the required task after the first access).

345 Again, in contrast, a privacy specialist from another Government agency explained the clear guidelines provided to staff on browsing client files. The same agency carries out monthly spot checks tracking the number of curious 'browsers' each year. Anyone caught browsing is provided with additional training, and disciplined if they repeat the behaviour.

346 Staff at ACC said they were too busy to browse random files. One call centre staff worker said, '[y]ou don't have time... half the time I don't even have time to check the [type] of injury, because you are so quick off the phone.' While we accept this at face value, it is nonetheless interesting that when asked about browsing no staff member responded that browsing would be a breach of privacy.

347 A lack of clear guidance and the absence of regular monitoring are a risky combination.

348 We also discuss how ACC's systems do not support ACC to run thorough checks and audits, including to identify 'browsing', in Part 7 (Systems).

Other examples demonstrating narrow definition of `breach'

349 While privacy is narrowly defined and the privacy team are actively focused on monitoring and measuring one kind of breach, staff can be relatively passive about privacy protection. There are systems, checks and balances in place to manage the risk of a staff member inadvertently sending a document to the wrong person. For example, before any email is sent externally a number of prompts appear on screen asking the staffer to confirm they intend to send the information. The strong systems in place to avoid this kind of breach explains why every interviewee defined a privacy breach in terms of 'sending an email to someone who should not receive it'.

350 But equally, staff are not necessarily alive to the possibility of other types of breaches. By way of example, one historical complaint to the OPC considered by this Review involved an email containing a taxi form was sent with an incorrect address in the form. This constituted a privacy breach because the address was that of another client. ACC's auto email check system did not identify this breach because the purpose of that tool is to check the identity of the email recipient only, as per ACC's narrow definition of what constitutes a breach.

351 In our view, a more proactive approach and a broader, more embedded privacy culture with the customer at the forefront, may help ACC to avoid incidents such as the Snapchat Incident in future.

352 It is worth noting that reporting by the OPC released in 2021 shows that human error was the leading cause of privacy breaches in the 2021 reporting period, with email error, data entry errors, accidental disclosure of sensitive personal information and postal and courier errors all examples of breaches caused by human error.[16]

353 ACC's privacy initiatives since the 2012 Independent Review have made significant progress towards avoiding privacy breaches by way of inadvertent disclosure. But a mature, embedded privacy culture would provide ACC with greater assurance to minimise all types of privacy breaches.

RECOMMENDATION: NARROW UNDERSTANDING OF BREACH

R8.6: Consider implementing an organisation-wide education programme on the many different way privacy can be breached, and take steps to ensure that this knowledge and understanding becomes as embedded in the organisation's culture.

Induction, training and reinforcement of training

354 ACC's privacy training module is titled 'Practice Privacy Protect People'. The Learning Management System **(LMS)** states that the module takes approximately 20 minutes to complete.

355 The module opens with a breach scenario, where Lily, a Recovery Team Member requests the medical notes from a client's (Henry) doctor in preparation for an assessment. The medical notes Henry's doctor sends through contain information about health conditions not relevant to Henry's injury, which Lily did not redact before she uploaded and sent the notes to the assessor.

356 The scenario then goes on to explain Henry's distress in seeing that information unrelated to his injury has been included and sent to the assessor. It explains that Henry had complained to the OPC and that ACC apologised for the privacy breach and paid Henry $10,000.

357 The scenario then goes on to state:

> Mistakes like this can happen easily. Providers and other agencies often provide ACC with more information than we need.
>
> It's important to clearly define the scope of your request when collecting medical notes and to read information carefully when it's received, redacting anything that isn't relevant to the claim.
>
> Sometimes information may be relevant to the claim but not to a specific type of assessor or provider. This is why we must complete a privacy and relevancy check of information at the point of disclosure, as well as when it is first received by ACC.
>
> Treat customer information as if it was your own — it's our responsibility to ensure New Zealand's trust and confidence in ACC by protected privacy breaches and keeping information safe.
>
> Practise privacy; protect people.

358 The privacy module has four separate pathways depending on what type of work the person completing the module does. The client information module is for people who handle client information, and notes 'you will often be faced with time pressures and are handling a lot of information, including health information, that you need to process quickly'.

[16] Office of the Privacy Commissioner 'Human error leading cause of privacy breaches' (1 December 2021) <privacy.org.nz>.

359 Participants are then guided through five scenarios which require them to identify how they would act in certain situations. All of these scenarios focus on avoiding a privacy breach, and are based on ACC's most common causes of privacy breaches, starting with selecting the incorrect provider in ACC's system, which is ACC's biggest cause of privacy breaches. These breaches typically see information which was meant to be sent to physio A, for example, sent to physio B instead.

360 The module concludes by noting:

> Remember the information we handle affects real people, like you. Treat it as if it was y our own.
>
> - Make sure you follow all checking processes, particularly when liaising with service providers.
> - Action requests for information as soon as possible.
> - Check emails before you hit send and always open and check attachments.
>
> Think about what you will stop, start and continue to help safeguard our clients' and customers' information.

361 The privacy modules confirm that ACC's privacy culture is driven by a desire to avoid breaches. The module starts with a story of a breach, rather than introductory statements about broader concepts such as what is personal information, why it is important to safeguard and protect personal information, and what ACC's statutory obligations under the Privacy Act are. Other than brief statements about how personal information is important, the rest of the modules are similarly focused on breaches rather than privacy as a concept and the idea that personal information is a taonga.

362 The impression of this Review is that the training modules appear inadequate and not sufficiently broad to be properly educational. It is concerning that new staff members can complete the training without actually completing the answers to the modules. We were told that these modules are the key documents staff would rely on to understand their privacy obligations, together with ACC's intranet page. At the same time, we were told by one interviewee that they worked for four months prior to completing the training.

363 In addition, while the modules purportedly require individuals to select particular answers before they are able to continue, trainees are in fact able to progress through the modules without answering the questions. One staff member we interviewed commented that you could 'cheat your way through [the modules]'. In addition, the answers are often fairly obvious (for example, the correct answer is the most detailed one) and, in our view, even if staff did answer the questions, it would be easy for participants to 'rush' though the modules without properly reading or considering them. That said, ACC does track completion of the modules (although there are no targets by which they must be completed) and staff receive regular email reminders if they have not actually completed the modules.

364 A review of screenshots of ACC's intranet page on privacy shows that it also has a focus on risk or operational matters - for example, guidance about what to do if you want to report a breach or are working on a project. From the screenshots we received, it appeared that the intranet page contains no high level values statement nor an expression of the importance of protecting privacy.

365 Many interviewees said that the staff involved in the Snapchat Incident would or should have known better because of the training they received and because of the Code of Conduct. Another interviewee who was familiar with the staff involved in the Snapchat Group commented that they did

not recognise that sharing information on a `work' Snapchat was problematic, despite the privacy training and other guidance they were given.[17]

366 In fact, all new staff receive limited training and the training does not provide basic guidance on the full range of privacy risks and protections. Given the turnover of staff, referred to above, this poses a constant and real risk.

RECOMMENDATION: INDUCTION AND TRAINING

R8.7: Undertake a comprehensive review of ACC's privacy training, including to address the gaps identified in ACC's induction and ongoing training. Such review should consider at least the following:

- Ensure privacy training modules and associated material (for example, the intranet page) adequately teach staff key values, including the importance of privacy and protecting personal information.
- Ensure privacy training covers all aspects of the IPPs — collection, retention, use, sharing, and disposal of personal information.
- Put in place annual refresher training (we understand that ACC, as part of its Improvement Initiatives, is currently considering a new approach to re-engagement activities, such as Privacy Week, but we would recommend that it actively consider annual refresher training in addition to re-engagement activities).
- Consider what additional training may be necessary for different types of staff. For example, younger staff members or employees that are new to employment or the public service may need more targeted or detailed training.
- Ensure all staff are required to actually complete privacy training and other modules within one month of commencing their employment at ACC.
- Remove the ability for staff to 'skip' through training modules so that all trainees are required to answer the questions posed by the modules.

Impact of working from home

367 As discussed in Part 3 (Overview of Snapchat and Access Incidents), much of the sharing at issue in the Snapchat Incident occurred while staff were working from home during the 2021 COVI D-19 lockdowns. More generally, we understand, as with many workplaces, COVI D-19 has led to an increase in the number of staff working from home across the organisation, and the frequency of staff working from home.

368 This introduces new privacy risks, particularly for call centre workers who talk and respond to clients. As noted above, when working in the office contact centre staff said that they would `vent' or debrief after a difficult call by talking to their team leader or, more often, turning to the person next to them. One staff member said:

> Ever since this whole thing came to light, we are not meant to talk to our co-workers. Like if we have a difficult call or something and you want to discuss it, you are meant to talk to your Manager. People still talk to their co-workers though, because I think sometimes you'll have a hard call or a funny email and it might just be a little something you want to say to a colleague and you don't feel like making a big deal out of it by pulling your Manager aside. You might just feel like, 'Oh, this person's quite frustrated for this reason'.

[17] We understand that ACC has now introduced refresher training following the Snapchat Incident.

369 While that staff member indicated they would anonymise the caller when talking to a colleague, they also readily acknowledged that there were occasions when it was obvious who was being discussed. For instance, when the caller is someone who calls frequently about the same injury or issue.

370 Contact centre staff told the Review they answer between 20 and 60 calls per day, and it is a challenging and isolating job. Some clients are distressed, or angry, and call centre workers need to manage whatever situation arises. One interviewee observed that, `there will be calls where someone has just abused me and the hairs on my neck will just stick up'. It is in this context that venting, or debriefing to a colleague is a natural response that allows staff to manage the stress of their job. One very experienced contact centre staff worker commented that from time to time she might put herself on a break and go for a walk, whereas 'a young staff member would vent'.

371 Working from home (whether during lockdown or by choice via a flexible working arrangement) means that staff can no longer turn their chair toward their neighbour and talk. It also means that it is more difficult to gauge how team members are feeling or managing their workload. One interviewee said:

> It is very easy to pick up in the call centre when someone is dealing with a difficult call because of the things they might be saying or you can tell they can't get a word in. So after the call, most of the time, people will come up and be like, 'Are you ok?'

372 ACC introduced daily Teams calls and other team building exercises to provide staff connection and support during lockdowns. These are positive initiatives but, for workers facing immediate stressors, they will never be a substitute for a colleague checking in on another colleague directly after a difficult call.

373 ACC needs to be alert to the fact that communication channels are important. When workers are working remotely:

a Staff need guidance and support to develop safe ways of debriefing after tough calls in a way that respects clients' privacy.

b Simply instructing that they must not discuss clients' personal information is not sufficient guidance, since when staff work from home they may need to give context about why a call was difficult and such context risks being identifying information.

c Telling staff to discuss difficult calls with their manager is unrealistic because managers will be busy and staff are likely to feel less comfortable contacting a manager from home than a peer.

374 Working from home will remain a part of the corporate landscape long after COVID-19 has left us. It is therefore important for ACC to ensure that it has a clear and comprehensive set of guidelines and principles in place to support staff working from home.

Callout culture

375 As discussed in Part 3 (Overview of Snapchat and Access Incidents), ACC first became aware of the Snapchat Incident when approached by the media for comment. This was because one of the members of the Snapchat Group contacted the media about the sharing that had occurred, rather than raising it internally. In light of this, we have reviewed the current mechanisms ACC has in place for staff to callout inappropriate conduct.

376 We understand from interviews and a review of documents that ACC has a system in place for reporting privacy breaches. One staff member we interviewed described the process as `vigorous'. The system requires staff to raise privacy breaches with their team leader, who is then responsible for reporting to the privacy team who log the breach (or near miss) into a privacy breach reporting tool on the intranet.

377 From the information we received from ACC, this reporting tool does appear to be widely used —there were 500 breaches reported in the 2020/21 financial year, and there have been 303 reported to date in the 2021/22 financial year (a review of the breaches shows that the majority of them were inadvertent disclosure breaches, such as sending information to the incorrect health provider).

378 In addition to the privacy breach process, ACC's Integrity Policy states that `all integrity incidents must be reported to Integrity Services or Talent'. It notes that guidance on speaking out is accessible on ACC's intranet and refers to an `Okay2Say' page. The Integrity Policy notes:

> We are committed to ensuring our people feel safe raising concerns, have trust we will act and provide visibility around decisions being made. Our people can raise a concern in confidence with an assurance anonymity will be maintained wherever possible.

379 The Integrity Policy is discussed in further detail in Part 5 (Policies and procedures).

380 When asked about how they would report incidents or concerns about the actions of their colleagues, staff interviewed said that they would likely report these to their Team Leader or Manager. However, none reported having ever done so and none referred to or acknowledged the existence of the Integrity Policy or the Okay2Say page. In our view, this demonstrates a lack of awareness and understanding of the formal processes in place to callout inappropriate behaviour.

381 This lack of awareness and understanding is also demonstrated by the information about Integrity Services reports we were provided with by ACC. This information showed that, in the five years prior to 2022, fewer than 10 reports containing allegations of inappropriate access to ACC systems that hold personal information were reported. Further, ACC concluded that the majority of the allegations were not substantiated without investigating them, and only two incidents progressed beyond the initial assessment phase.

382 In our view, the fact that the individuals involved in the Snapchat Incident did not raise their concerns internally before approaching the media demonstrates a disconnect between the callout culture on paper and in practice.

383 When speaking about the impact that the media reports of the incident had had, one staff member said:

> ...what about all of these people now that we've lost. Those people that will never come forward to us now. And what we offer by way of sensitive claims is phenomenal in terms of services and that kind of thing and they'll never come and we've got no opportunity now to find them, speak to them, bring them in.

384 A stronger, more embedded callout culture may have enabled ACC to identify the issue before it was publicised by the media. In turn, this may have helped to protect ACC's most vulnerable customers from the distress of thinking that their personal information was being shared in such a way.

385 ACC has advised that reviews of the Board's governance now include regular reporting on `speak up' matters. This is a good first step.

RECOMMENDATIONS: CALLOUT CULTURE

- **R8.8:** Complete a detailed review of its callout culture (in addition to the review of its Integrity Policy recommended at **R5.5** and **R5.6)** to ensure that there is a robust system in place to enable staff to raise concerns anonymously and without fear of retribution.
- **R8.9:** To better ensure that all breaches and near misses are reported, ACC's review of its callout culture should consider what changes can be made to the privacy breach reporting tool to ensure staff are aware of the different types of breaches that can and should be reported.

Use of social media

386 Call centre staff of all ages acknowledged that they used informal platforms like WhatsApp and Facebook Messenger to keep in touch with colleagues, particularly during lockdown. They used the social media channels to share photos and news about their weekends, their gardens and other non-work activities, or to communicate with one another when they had trouble accessing ACC systems. Such informal communications groups are being used by staff to develop friendships and connection. Staff report these channels are an extension of their working relationships, although some of these groups include former ACC staff.

387 In these circumstances, it is easy to see how such informal channels could include references to work calls and work stressors. At the same time, the kind of information shared by the Snapchat Group went well beyond what other staff report is or would be shared on social media.

388 Banning the use of such channels or even banning the use of personal devices during work hours is not a solution. Informal social media channels will continue to be a part of how everyone communicates and it is, therefore, more important that the policies ACC has in place and the culture it builds support appropriate use of them. Again, proper induction and on-going training will be key. In terms of client personal information, personal devices are as safe as the staff who control them. If ACC staff have a proper understanding of what privacy means and are taking responsibility for the protection of all client information, as they should, then any risk is reduced.

389 One issue raised during the Review, which we record for completeness, was the possibility that younger staff may be more likely to use social media and may have different privacy settings than older workers. All of the staff involved in the Snapchat Incident were aged under 30.

390 One interviewee noted:

> Peoples' idea/concept/value of privacy is entirely different for millennials or Gen Z's versus others. I think we are going to have to constantly battle and embed and refresh culture that looks at that and seeks to lean into it.

391 Whether younger people do, in fact, have different privacy settings is a topic that has not been fully settled by researchers. Having interviewed staff from across a range of ages we discerned no noticeable difference in either their understanding of privacy or the way they described ACC's privacy settings. Throughout the Review there was a high degree of unanimity in the views expressed, irrespective of age, position, geography or experience.

392 We discuss ACC policies in respect of personal devices and social media, and make recommendations regarding these, at Part 5 (Policies and Procedures).

Other cultural factors

Next Generation

393 As set out in greater detail in Part 7 (Systems), Next Generation is ACC's new approach to managing claims that was rolled out between July 2019 and September 2020.

394 Among the many changes brought in by Next Generation, the new system has resulted in a change in approach whereby (for the majority of claims) no one single staff member 'owns' a claim or a client. Instead of working on a set number of claims at any one time, staff now work on 'tasks' that are auto-assigned by the system.

395 This means that there are many more 'hands' (or eyes) across a file at any one point in time. It also means that a greater percentage of the work done on an ACC file is automated. We understand that this creates many efficiencies for ACC and faster response times for clients. More urgent tasks are given priority and there is less downtime while staff wait for a development or task on an assigned claims.

396 However, increased efficiencies can have a negative effect on an organisation's privacy culture. Some staff we interviewed, including from the privacy team, commented that there had been a rise in low level breaches since the introduction of Next Generation. One privacy team member noted that this may be due to the change from a single person having responsibility for a file to a many hands approach. Many hands means more occasions for small mistakes to be made and less sense of ownership or responsibility.

397 Other staff rejected this premise, however. One noted that Next Generation gave ACC better visibility and transparency of certain datasets, which was why the number of reported breaches had risen —because ACC was better able to identify that a breach had occurred now.

398 In our view, and based on the comments of staff working on the ground, the introduction of Next Generation is likely to have impacted ACC's privacy culture and in turn may have contributed to a workplace culture in which incidents like the Snapchat Incident are more likely. In particular:

a the system's increased automation removes tasks that would previously have been manually completed from staff's control. Where an increasing amount of a person's work is automated, they are likely to be less alive to privacy risks;

b the system encourages staff to meet daily quotas of tasks completed. Staff's performance is measured against these quotas. This puts an emphasis on the tasks rather than the client (noting that clients are listed as claims, rather than people);

c the change from staff working on claims to staff working on tasks creates a greater separation between staff and the customer. This further exacerbates the problems discussed from paragraph 402 below, as staff are less able to develop a sense of connection to their customers when the customer is defined by the task and staff move at speed from one task to the next; and

d this method of processing client requests does not encourage or support individual staff having ownership and responsibility for protecting personal information. A shift in focus to have the

customer at the forefront of an ACC staff member's mind may help to build a stronger privacy culture. It is much easier for staff to feel a sense of connection to and protection over a customer than, for example, a concussion claim.

Turnover

399 Several staff we interviewed commented that ACC had a high degree of 'churn' and organisational personnel change. It was suggested to this Review that such consequences may be a result of not only the changes introduced by Next Generation, but also ACC's frequent organisational restructures. One person who had worked in the public service for a long period felt that ACC had a higher amount of restructure and organisational change than other public sector agencies.

400 The Review identified that two of the teams at the core of the Incidents experienced particularly high churn — being the contact centre and the privacy team.

a As at 24 January 2022, approximately 50% of ACC's contact centre staff have worked at ACC for 12 months or less.

b The Head of Privacy role has changed three times in less than two years, and at the time this Review was conducted there remained a number of vacancies in the privacy team. One interviewee commented that the privacy team had been 'relatively volatile' in terms of staff. Stabilising this team and setting conditions for its members to develop expertise and standing in the organisation should be a priority.

401 Outside these two specific teams, constant organisational change makes it difficult to build and mature a values-based culture. When staff are being continuously onboarded, the focus is, quite naturally, on basic induction and training. In the current climate, this is likely to be an on-going challenge for the organisation. Having a clear, transparent privacy roadmap (as discussed in Part 7 (Systems)) will assist both in the initial induction of staff, but in on-going development and cohesion.

Focus on `claims' rather than clients

402 It was starkly noticeable that ACC staff refer to 'claims' rather than clients.[18]

403 We consider that this is driven, at least in part, by ACC's continued efficiency drive. Working on a claim has easily measurable targets and progress markers that can be ticked off as the claim is assessed, accepted and various steps are completed. The focus may also reflect a change following the introduction of Next Generation, as discussed above from paragraph 393.

404 This is also reflected in the approach taken by the Annual Report. One of the key strategic intentions for ACC is to improve customers' outcomes and experiences, and ACC records data on levels of public trust and confidence and client trust score. It also records rates of return to work and return to independence for those not in the workforce. While these goals are important and reflect an intention to focus on customers, the Annual Report measures outcomes in terms of targets (which are met or not met) rather than using language which centres on the customer themselves. Phrasing the information in this way reflects a KPI focused attitude, based on the progress and outcomes of the claim rather than the individual who has made the claim. For example, Table 19 on page 113 of the

[18] The exception to this is the work done by staff working on sensitive claims. We received a clear and strong impression that they understood and valued each and every client they worked with.

Annual Report presents claims data relating to claim outcomes in terms of numerical targets which have been achieved or not achieved rather than talking about the customers who form the basis of the claims.

405 In our view, this contributes to ACC's narrow privacy culture because staff working on claims are thinking about a claim — that is, an individual's claim for a concussion, rather than the individual themselves.

406 Where a claim is separated from the customer, it is easier for staff to lose sight of the customer and in doing so lose sight of the importance of protecting that customer's personal information. This is natural — ACC staff work on many claims at any one time, and that volume of work means staff can become desensitised.

407 We consider that a shift in focus to have the customer at the forefront of an ACC staff member's mind, may help to build a stronger privacy culture. It is much easier for staff to feel a sense of connection to and protection over a customer than just another concussion claim.

RECOMMENDATION: FOCUS ON CLAIMS RATHER THAN CLIENTS

R8.10: Consider how to shift the focus from claims to clients across corporate documents, training and performance measures, to ensure that the client or customer is always front and centre (and recognising that language is an important tool to embed values).

Sensitive claims

408 As further described in Part 7 (Systems), ACC uses EOS 'tags' for the handling of, and access to certain types of claims - sensitive claims, VIP clients, RCU clients, and staff files. Recent work that ACC has done on role mapping and restrictions on access (see Part 7 (Systems)) has ensured that only certain staff members can access sensitive claims (and there are further restrictions in place for VIP clients).

409 During interviews we were given the impression that ACC staff consider that these restrictions in place will help to ensure that the wrong staff can't access sensitive information. As noted already in this Review, repeatedly interviewees communicated that any sensitive information held by ACC was contained in the sensitive claims. This is clearly false.

410 The language used to define categories of claims appears to have, inadvertently, contributed to staff's poor understanding that personal information is a taonga. It may also have contributed to staff handing some kinds of personal information with less care than other kinds of personal information. Much of the information ACC holds is sensitive. Beyond the information held on its sensitive clients, client files contain information about traumatic brain injuries, injuries that have resulted from horrific (non-sexual) crimes, birth injuries and other psychological injuries. Even information about a basic whiplash may be sensitive to an individual because of how that injury occurred or the challenges a person has faced to have it treated.

411 We have therefore recommended that ACC reconsider the language used to describe its sensitive claims, to ensure that it remains clear to all staff (and to the public) that all client information held by

ACC is (or can be) sensitive. Such a shift in understanding will be required if ACC's privacy culture is to be strong and mature.

RECOMMENDATION: SENSITIVITIY OF INFORMATION

R8.11: Give consideration to how the word 'sensitive' is currently used to denote personal information that requires additional legal protection. In staff induction and training, consider how to provide education on the fact that all personal information, not just `sensitive' information has and requires legal protection under the Privacy Act and other legislation.

Schedule 1

Terms of Reference

Schedule 1 Terms of Reference

The Review is sought to provide recommendations on effectiveness and improvements following public attention on two specific issues:

- The number of ACC staff who may access client files; and
- Alleged inappropriate access and use of client information among ACC staff.

The Review will address:

The issues arising from the recent alleged inappropriate access and use of client information among ACC staff and resulting privacy breaches; and

A Review of:

a Systems and policies in relation to access to and use of client information among ACC staff (including the potential for inappropriate use of client information including employee browsing and inappropriate access and use of client information among staff).

b The oversight, monitoring and auditing of access and use (to detect and deter unauthorised access and use of client information) and, whether they are sufficient and fit for purpose to detect and deter the incidents described in item 1 above.

c Ongoing training related to such access and use of client information.

The review will provide recommendations where improvements can be made to systems, policies, oversight, monitoring and auditing activity and training in order to strengthen public confidence in ACC's ability to manage client information securely and with respect for the privacy and dignity of their clients' personal information.

1 **Background**

Privacy and appropriate access to and use of client information has been, and is of, central concern to ACC and existing policies are in place. All new staff receive training regarding the appropriate way to handle information and this training is ongoing.

Any breaches of policies concerning the access to and use of client information are taken extremely seriously.

In recent weeks, concerns have been raised publicly about the number of staff who are able to access client files and about the access and use of client information among staff. ACC management has reviewed policies concerning access to client information and where client information has been shared, staff have been stood down while further investigations take place.

However, concern has been raised among members of the public about the way client information is handled by ACC as described in item 1 for the Review above and, as such, the Board has requested an independent review be undertaken as outlined above to ensure the public has confidence in how ACC manages client information.

The following are of potential relevance to the Review:

- The number of staff who have access to client files and the reasons for that access; and
- The impact on internal security of the recent changes in the way sensitive claims are administered; and
- Whether the systems have the ability to provide more limited or role-based access to certain types of claims or levels of data/information.

2 Scope of the Review

ACC will continue with its current investigations into the recent alleged inappropriate access to and use of client information as a matter of urgency. ACC's employment relations investigations and decisions are out of scope for the reviewer but there is an opportunity to review ACC's response for its appropriateness and to capture any insights relevant to this Review.

The objectives of the Review will be to:

- carry out an overarching review of the issues raised by the recent alleged inappropriate access to and use of client information as described in item **1** for the Review above (and having considered the causes, including examining the potential impact on internal information security of the recent changes in the way sensitive claims are administered);
- make recommendations to the ACC Board about appropriateness, effectiveness and how to improve;
- systems and policies in relation to access to and use of client information among ACC staff;
- the oversight, monitoring and auditing of access to and use of client information (to detect and deter unauthorised access and use of client information as in the incidents described in item **1** above); and
- the ongoing training related to such access to and use of client information.

Excluded from the scope of the Review is any review, investigation, commentary or findings of fault regarding any individual at ACC or any employee investigations and outcomes and, accordingly, also excluded is any consideration or recommendation of any disciplinary, civil or criminal action to be taken. These matters will be addressed by ACC as an employer of ACC staff.

3 Roles and Responsibilities

In order to ensure that the Review has the appropriate powers to complete a thorough investigation, a partnership between the ACC Board and the Treasury (as ACC monitor) is proposed. The partnership between the ACC Board and the Treasury aims to achieve a structure that is enabled by the powers of the ACC Board and the independence of the Treasury as monitor. Under the RACI structure:

ACC Board	Responsible and Accountable
Treasury (as ACC monitor)	Responsible
Minister for ACC	Informed

The Senior Responsible Officer (SRO) for the Review will be Vanessa Oakley, Chief General Counsel of ACC, reporting to Steve Maharey, Board Chair of ACC for the purposes of this Review. The SRO will put in place an ACC support team, including resource from ACC to engage with the Review and to comment on a draft report.

Carolyn Palmer will be the Treasury's responsible officer for the Review and will work in partnership with the SRO at key stages of the review, signing off the Terms of Reference, comments on a draft report and enabling resource from the monitoring team to engage with the Review as appropriate.

The Privacy Commissioner will be offered the opportunity to be consulted during the review and on the draft report. Issues that arise during the Review could also create an opportunity for consultation with the Privacy Commissioner rather than waiting for the draft report.

ACC and the reviewer will develop procedures to protect personal information of individuals (including staff and clients) and ensure that confidentiality in such information is maintained during the investigation and in the report.

The Minister for ACC will be informed about the Terms of Reference and the final report before these are publicly released.

4 Leadership of the Review

The Review will be led by Linda Clark, with support from Dentons Kensington Swan.

ACC will provide access to the following as are relevant to the scope of the Review:

- Policies and systems.
- Related training material.
- External and internal risk, assurance and audit reports.
- Briefings from key staff in relation to the above.
- Other requests or access to staff to be agreed.

5 Timing

The review will be conducted over a maximum six-month period starting from mid November 2021. A detailed project scope and timeline will be confirmed by the Reviewer once these Terms of Reference have been finalised with the Reviewer. Delivery against the timeline will be subject to availability and access to all relevant information.

6 Deliverables

The key deliverables of the Review to the SRO include the following:

- Regular feedback on findings as the Review progresses.
- A Draft report, enabling ACC and Treasury to provide comment.
- A final report following consideration of ACC and Treasury comments.

In conducting the Review, the reviewer will comply with all applicable laws, including in relation to personal information.

7 Publication

The expectation is that the final report (subject to any redactions) will be available for public release. ACC will have the opportunity to review the final report and make redactions for publication (including if required to manage privacy, commercial sensitivity, or security concerns). Treasury will be engaged on this process to ensure redactions do not conflict with the public interest. The details of the report should be kept in strict confidence until ACC and the Minister for ACC have determined the timing to release the final report.

Schedule 2
Client information journey at ACC

Schedule 2 Client information journey at ACC

Information journey

1 While this Review sought to develop a clear picture of the information 'journey' at ACC, we were not provided with a clearly documented information 'map', nor could anyone that we interviewed provide us with a clear picture.

2 At a very high level, based on the information that we were able to ascertain during the Review, the client information journey within ACC is as follows:

a The client is injured and visits a treatment provider (for example, a physiotherapist or the ED of a hospital).

b All claims start with the provider (and client) completing and submitting an ACC45 Injury Claim Form (ACC45 Form) or similar initial claim documentation.

c In some cases, ACC will receive sensitive claims via a 'Sensitive Engagement Form' (submitted by providers who are party to an integrated service for sensitive claims contract with ACC, such as psychologists and psychiatrists). That form is submitted digitally, and automatically identified as a 'sensitive claim' by ACC's systems (see further comments on access to sensitive claims below).

d The initial form documentation is sent to ACC (either electronically through a gateway established by ACC, or manually). Information and documents received by ACC (including initial claim documentation) are, subject to checks carried out by the inbound document team, uploaded to EOS (ACC's client management system, discussed further below).

e When the claim enters EOS, an 'engagement management decision' tool (EMD) is automatically applied to every claim (with the exception of claims coded as sensitive). The EMD is essentially a sorting algorithm, based on business rules and statistical models to determine the level of support required. EMD automatically matches claims to the appropriate client engagement team. Where a claim cannot be matched through this automated process, ACC personnel will manually triage the claim.

f If EMD determines that the client is clearly eligible for the entitlements sought (and the injury and entitlement are not complex in nature), those entitlements are automatically approved without need for further engagement with ACC. The vast majority of claims made to ACC are automatically approved through this process. No claims are declined using EMD. Claims resolved through EMD are typically not seen by any staff member (that is, no person physically looks at the claim), although the claim remains in ACC's EOS system.

g Those claims which cannot be automatically resolved through EMD, are triaged according to guidelines provided by Next Generation (described further in Part 7 (Systems)). The categories of triage are defined internally by ACC as follows:

i **'Enabled recovery'** is where the client will primarily manage their own recovery using ACC's self-service tool, MyACC, to select services and request support. Clients in enabled recovery are not assigned a dedicated case manager so if they call ACC for any reason, they could be managed by any call centre worker on duty at that time. An example of a client who may receive this level of engagement is an office worker with a fracture, who can still work most of the time.

ii **'Assisted recovery'** is where the client will primarily manage their own recovery, but ACC will contact the client if there is something specific to discuss (for instance, where additional services are required to progress recovery). An example of a client who may

receive this level of engagement is a teacher with a dislocated shoulder who may need additional services, such as help travelling to and from work.

iii **'Supported recovery'** is where the client is assigned a dedicated ACC contact who supports their recovery, for instance, to manage multiple treatment providers and additional services as required. An example of a client who may receive this level of engagement is a farmer with a disc prolapse, who receives support from multiple treatment providers possibly over a longer time period, and who is recovering while working in a challenging work environment.

iv **'Partnered recovery'** is where the client is assigned a dedicated ACC contact, and it is anticipated that the client will need support for an indefinite period due to the complexity of their injury and need for (potentially) life-long support and partnership. An example of a client who may receive this level of engagement is a client with paraplegia, who requires expert support to coordinate specialised services over a long period.

v **'Provider managed'** is where the client is supported by treatment providers (rather than ACC) who work with them to manage their recovery. An example of a client who may receive this level of engagement is a client with an ACL rupture where the pathway for treatment is well understood and established.

h Where a claim is triaged to one of the recovery teams, the client will be contacted by a member of ACC's recovery engagement team for what is referred to as a 'welcome conversation'. The purpose of this conversation is to discuss the client's treatment, to introduce the client to the MyACC self-service tool and to obtain verbal authorisation by or on behalf of the client so ACC can collect further personal information.

i For as long as the client's recovery remains under ACC management, further documents may be requested by ACC and/or provided by the client and/or treatment providers. Any documents received are checked by ACC's inbound documents team and (subject to those checks) inputted into EOS. EOS remains the primary 'source of truth' database for client information across the lifetime of a claim. Depending on the complexity of the claim and the length of recovery, an EOS file on any client may contain a large amount of information from a wide range of different treatment providers and health professionals.

i ACC may also request further information directly from the client, for example, through the welcome conversation (conducted by ACC personnel and the client) or information submitted by the client through the MyACC self-serve portal. In some cases, ACC will use standardised forms and consents to obtain further information about clients. For instance, in the case of sensitive claims, ACC obtains ACC6300 consent from all clients, submitted by their provider at the same time as the 'early planning report' is provided (after six sessions of therapy).

k For the most part, claims (and all information, files, and documents associated with that claim) are retained by ACC for up to 75 years following the last action on the file in accordance with ACC's retention policy.

Categories of information

3. The following table summarises the categories of client information held by ACC and the source of that information:

Type of information	Source of information
Personal details, such as the client's name, date of birth, home address, contact numbers, gender, and ethnic background	Provided by: • the client and/or the treatment provider in the ACC45 Form submitted to ACC. • the client during the welcome conversation with ACC. • the client through MyACC.
Injury and medical details, such as: • Details about the accident, including the date, time, accident scene, accident location, and cause of accident. • The client's NHI number. • The 'diagnosis read code'. • Whether the injury is a gradual process injury. • Whether the claim is for medical misadventure. • Recovery goals. • Psychological and physical therapy interventions. • Relevant medical records or assessments capturing information, such as the client's mental health, home-life and daily living needs, transport and housing needs, work capacity (the hours the client is able to work, restrictions, and capacity for job types). • Treatment provider referral details and treatment objectives. • Information about whether the patient is able to continue normal work (or work with restricted duties, and for what period). • Information about whether a review is required for the client to return for work or the particular date that it is anticipated the client will be fit to return to normal work.	Provided by: • the client and/or the treatment provider in the ACC45 Form submitted to ACC. • the client during the welcome conversation with ACC. • the client through MyACC. • the client's treatment provider(s), including through assessment reports (if applicable, for example, the 'Stay at Work' report). • the client's GP or a nurse practitioner to ACC through the submission of an ACC18 medical certificate (used to certify that clients are unfit for selected duties and to outline the types of work that the client can carry out with their injury).
Employment and tax details, such as: • Name and address of the client's employer at the time of the accident. • Occupation. • Earner status.	Provided by: • the client and/or the treatment provider in the ACC45 Form submitted to ACC. • the client during the welcome conversation with ACC. • the client through MyACC.

Type of information	Source of information
• Work type. • Whether the accident occurred at work. • Liable earnings. • IR number. • Bank account details. • Full work history. • Relevant work skills, training, and experience. • Details about the client's employment (including type of work and name and address of business).	• Inland Revenue pursuant to information sharing arrangements with Inland Revenue. • the client's employer. • the client and/or treatment providers in the context of an occupational assessment.
Third party information, such as: • Treatment provider information, including the provider's name, contact details, ID, facility and vendor address, and provider/vendor/supplier bank account information. • The name and contact details for the client's legal representative and/or advocate. • The name and contact details for parents of clients aged under 16 years. • The name, contact details, and living situation of other parties associated with a claim, for example, the client's surviving spouse.	Provided by: • the client and/or the treatment provider in the ACC45 Form submitted to ACC. • the client during the welcome conversation and 'recovery check in' phone calls with ACC. • the client through MyACC. • the client's treatment provider(s), including through assessment reports and medical records.

Schedule 3
Summary of media reports

Schedule 3 Summary of media reports

The following table summarises the Radio New Zealand reports released in 2021 in respect of the misuse of information within ACC (including the Snapchat Incident and the Access Incident):

Date	Article title and lede
9 August 2021	**Overwhelmed ACC staff 'dropping like flies' after changes** *A budget-blowing restructure of the way ACC manages claims has left staff with "overwhelming caseloads" and so stressed they're "dropping like flies", a Public Service Association (PSA) union survey has found.*
30 September 2021	**ACC admits backlog is delaying tens of thousands of client cases** *ACC is struggling to clear a month-long backlog of work, with some tasks more than seven months overdue, the organisation has told MPs.*
12 October 2021	**Man horrified 92 ACC staff accessed his sensitive claim file** *A man disabled by a workplace accident is horrified dozens of ACC staff looked at his sensitive claim file on childhood sexual abuse, viewing it more than 350 times after it was closed. The file of his wife, who acts as his advocate, was also accessed. The couple say their rights and privacy have been breached, but ACC says every access was justified.*
13 October 2021	**Check which ACC staff have accessed your file, abuse survivors urged** *There is a widespread and systematic problem of ACC staff having inappropriate access to the files of sexual abuse survivors, advocates say.*
27 October 2021	**ACC staff posted clients' details to Snapchat group** *ACC call centre workers shared details of people's injuries and mocked them on Snapchat, RNZ can reveal.*
15 November 2021	**ACC whistle-blower surprised not to hear from investigators** *An ACC employee who blew the whistle on call-centre staff sharing and laughing at client details in a private Snapchat group says no one from the agency has been in touch with them about the matter.*