methodist themission

INFORMATION SHARING AND HIGH NEEDS CLIENTS:

An assessment of practitioner, manager and organisational competency relating to privacy principles and the sharing of personal information of clients pursuant to principle 11 and part 9A of the Privacy Act 1993

ACKNOWLEDGEMENTS

This research was supported by the Office of the Privacy Commissioner.

Thank you to all respondents and participants who gave their time, stories and insights and Mission staff who assisted with the project.

Ehara taku toa i te toa takitahi, engari, he toa takitini –
Success is not the work of one, but the work of many

A Report for Methodist Mission Southern

(Kayla Stewart (Researcher) & John Crawford-Smith)

TABLE OF CONTENTS

EXECUTIVE SUMMARY

It is often necessary to share information in order to provide comprehensive and wraparound services for clients. Positive outcomes for clients may be inhibited and the effectiveness of services compromised when information that should be shared is not. The ramifications of not sharing information may be significant with a lack of information sharing being cited as a contributing factor in several high profile family violence and child abuse/neglect cases. While recognising information sharing is very important, it is also necessary to protect and uphold the privacy rights of clients. Hence agencies and practitioners are required to strike the delicate balance between sharing and protecting client information.[1]

The Privacy Act 1993 (the Act) is the primary piece of legislation that controls the protection and disclosure of information. At the core of the Act are 12 privacy principles (hereafter, the principles) that govern the collection, storage, access and correction, accuracy, retention, use and disclosure of personal information. In order to facilitate increased information sharing, the Act was amended in 2013 to create a new legal framework, known as Approved Information Sharing Agreements (AISAs) which provide a mechanism for information sharing amongst certain government agencies.[2] There are currently three AISAs in place: Information sharing agreement between Inland Revenue and the Department of Internal Affairs, Information sharing agreement between Inland Revenue and New Zealand Police and Information sharing agreement for improving public services to vulnerable children.

This report was funded by the Office of the Privacy Commissioner and examines practitioner and organisational competency across a range of agencies relating to the principles with a specific focus on the sharing of personal information pursuant to Principle 11: *Limits on disclosure of personal information* and Part 9A: *Information sharing* (AISAs) of the Privacy Act 1993.

A mixed-method design was used whereby surveys and semi-structured interviews were undertaken. In total, 146 completed survey responses were collected and 20 interviews conducted. In order to obtain frontline and organisation level perspectives, two surveys were administered: one for practitioners and the other directed at senior practitioners/managers. Both managers and practitioners took part in interviews.

Methodist Mission Southern (The Methodist Mission) conducted the research. The Methodist Mission is a multi-disciplinary social service agency that has been operating throughout Dunedin and Otago since 1890 (for more information on The Methodist Mission, see Appendix One). Drawing on The Methodist Mission's networks enabled the survey to be circulated to a wide-range of organisations and access to a set of participants who interact with high needs clients.

[1] For the purpose of this report, the terms 'agency' and 'organisation' are used interchangeably.
[2] Privacy Amendment Act 2013, s 11.

Analysis of the data produced numerous findings including:

- The majority of organisations received requests for client information and most practitioners have shared information with another organisation within the last 12 months with more than a third having done so 21 or more times. Most of the requests are from clients themselves and government agencies.
- Nearly one third of practitioners report not being trained in the Act and the principles. Of the participants who had received training, some considered the training to be inadequate.
- Few practitioners find the principles easy to apply in practice.
- There are practitioners and managers who mistakenly believe that when sharing information, withholding a client's name but still providing identifiable details means they are complying with the Act.
- Not all organisations are training staff members on when other legislation or formal Memorandums of Understanding that concern sharing client information may apply (NB: The Privacy Act 1993 is 'trumped' by other legislation).
- The majority of organisations have an information-handling policy and staff members are able to access it.
- Just over half of organisations are complying with their obligation to have a privacy officer. The majority of practitioners do not know who the privacy officer at their organisation is. As stipulated in the Act, as well as dealing with information requests from clients, the privacy officer is required to ensure and encourage compliance with the Act. If no one is fulfilling this role, it may be that the organisation falls short in this regard.
- Few privacy officers reported undertaking training offered by the Office of the Privacy Commissioner.
- Over one third of practitioners surveyed either strongly agreed or agreed with the statement "Information sharing between organisations should only be allowed with the informed consent of the client (i.e. even if the Privacy Act 1993 permits the information to be shared without consent)". This belief was shared by some interview participants, who explained that doing so helped to build and maintain a trusting and transparent relationship with the client.
- Nearly half of practitioners have experienced a lack of response from other organisations when requesting information about a client.
- Nearly three quarters of organisations have a formal system for managing information requests but less than half have a system to ensure a response to an information request is made in the required timeframe. Less than half of organisations that participated are meeting the timeframe required.
- Less than half of practitioners reported being required by their employer to consult with another staff member (i.e. supervisor, manager, privacy officer) about whether client information can be disclosed. This is indicative of non-compliance with the Act as dealing with requests made to an agency is the responsibility of the privacy officer and it is their role to ensure compliance with the provisions of the Act. Furthermore, if practitioners are not being trained or their training is inadequate, this means information may be mistakenly disclosed or withheld. However, as most organisations require staff members to undertake this consultation it appears there

is a disconnect between organisational expectation and what practitioners actually do.

- From discussion with Māori providers, it was suggested that the Act is at times incongruous with a Māori worldview particularly in regards to information being collectively owned by whānau and the Act is often being breached to give effect to this.
- Challenges to information sharing primarily centred around the inability to share information when it was believed doing so would benefit the client, information being withheld when it was believed sharing would benefit the client and not knowing who to share information with.
- Some organisations and practitioners feared sharing information in case it places them in breach of the Act.
- Some participants described encountering situations where they thought the Act was being used as an excuse to refuse information sharing requests.

The following table provides a summary of the findings in relation to the associated privacy principles.

Principle 1: *Purpose of collection of personal information*	Most organisations have a policy about what kind of information staff may collect from clients however some do not, which means potentially unlawful/unnecessary information is being collected.
Principle 3: *Collection of information from subject*	Practitioners are not always explaining why they are collecting personal information to clients despite most organisations requiring them to do so.
Principle 5: *Storage and security of personal information*	Nearly all organisations have a policy about how information is stored and organisations and practitioners are aware of the practical elements required in terms of keeping client information safe. However, many organisations are not conducting audits of the IT security of client information. Thus, the potential exists for data breaches and client information being stored unsafely.
Principle 6: *Access to personal information*	Most practitioners are confident when it comes to identifying when they are able to give a client their own personal information but fewer are confident at identifying the circumstances when a client's own personal information can be withheld.
Principle 7: *Correction of personal information*	Nearly one in five practitioners is not confident regarding what to do should a client wish to correct their personal information.
Principle 8: *Accuracy, etc, of personal information to be checked before use*	Few participants reported checking if information acquired informally (such as "informal chats" or "little conversations" between other professionals and with the public) was accurate.
Principle 9: *Agency not to keep personal information for longer than necessary*	Most organisations have a policy relating to when client information is no longer required.
Principle 11: *Limits on disclosure of personal information*	Nearly one third of practitioners are not confident in knowing when the Act permits them to disclose a client's personal information. Many participants described getting consent from the client prior to sharing information. However, informal information sharing (without consent) was still prevalent with participants describing this practice as a way to acquire useful information about a client. Not being able to share information with family members when a client did not consent was cited as a barrier to positive client outcomes.

	Participants were generally well-informed when it came to knowing that they were able to disclose information in cases of a serious threat (also outlined in Principle 10). Many described this threat as needing to be 'imminent'. However, the threshold was amended by the Privacy (Information Sharing) Bill 2011 and 'imminent' was removed.
AISAs	One-third of practitioners have used their organisation's AISA to share client information but one-quarter did not know whether they had done so. The majority of practitioners are not receiving any instruction/training from their employer on how to ensure compliance with their organisation's AISA and only half have been issued with guidelines. This is indicative of non-compliance with the terms of the Approved Information Sharing Agreement for Improving Public Services for Vulnerable Children. Three-quarters of practitioners do not know what an 'adverse action' in terms of an AISA is. This is particularly concerning given that should an adverse action (including any action that may adversely affect the rights, benefits, privileges, obligations, or interests of any specific individual)[3] be identified, the terms of the Information Sharing Agreement for Improving Public Services for Vulnerable Children outlines steps to be taken. No practitioner considered sharing information with other agencies under an Approved Information Sharing Agreement to be easy.

Conclusions and recommendations

The findings show that both agencies and practitioners are conscious about the need to protect client information but at times there is noncompliance with the principles. Furthermore, there are various challenges faced at both organisational and frontline levels in terms of privacy and information sharing.

Some issues identified in this report may be ameliorated by proposals suggested following the Modernising CYF Expert Panel review. This includes the implementation of "a new high-trust information sharing system that is connected across agencies, partners, families and caregivers, brokered by a Child Information Management system, with a consent-based approach" (p. 122).[4] This would be in addition to the reformation of the Child, Young Persons and Their Families Act 1989 to create an information sharing framework which results in an expectation of access to personal information necessary to promote the safety and well-being of children and young people as well as protecting anyone acting in good faith from any civil or criminal action, or any professional disciplinary action. It is recommended that similar changes to the Privacy Act 1993 are considered.
Recommendations to address noncompliance of the Act include:

[3] Privacy Act 1993, s 97.
[4] Modernising Child, Youth and Family Expert Panel. (2016). *Expert Panel Final Report: Investing in New Zealand's Children and their Families* (pp. 1-300) (New Zealand, Ministry of Social Development). Wellington.

- Agencies have appropriate staff training in place so all staff who encounter personal information are trained in the principles and other relevant legislation or formal agreements concerning information sharing.
- Explicit instruction be given by agencies to staff about how informal information sharing is a breach of the Act and agencies implement processes to combat this.
- Agencies conduct regular audits of IT security of client information and informed of the technology guidance section on the Office of the Privacy Commissioner website.
- Agencies be advised of the requirement to have a privacy officer and staff made aware of who the privacy officer is and their role.
- The benefits of having someone in the role and the training for privacy officers available through the Office of the Privacy Commissioner be promoted.
- Education occur at an operational level whereby agencies and practitioners are taught their obligations under the Act, how to meet and incorporate them into policies and culture.
- Agencies to be informed of the resources on the Office of the Privacy Commissioner website as part of this process.
- The issues raised regarding a Māori worldview and privacy warrant further exploration.
- All staff members working under AISAs to be comprehensively trained in their use.
- Agencies and practitioners utilise the AISA guide 'An A to Z of Approved Information Sharing Agreements (AISAs)' produced by the Office of the Privacy Commissioner.
- Funding be invested into resourcing a more useable system to allow for and encourage information sharing under AISAs and the inclusion of non-government organisations as parties to the agreements be considered.
- That short 'go-to' guides on information sharing and certain privacy principles are produced. The guides should be written in a manner that is easy to understand (i.e. avoid legalese), utilise case studies and possibly flowcharts. The guides should incorporate resources already available on the Office of the Privacy Commissioner website. **Note:** reference guides and other resources have been developed as part of the research terms of contract.

INTRODUCTION

The keystone piece of legislation safeguarding and restricting the sharing of client information in New Zealand is the Privacy Act 1993 (hereafter, the Act). The overarching purpose of the Act is "to promote and protect individual privacy".[5] This objective is guided by the twelve information privacy principles as outlined in section 6 of the Act and pertain to the use, collection, storage and disclosure of information about a person (personal information) (see Appendix Two). The Act applies to "agencies"[6] – essentially any individual, organisation or business that holds personal information[7] in both the public and private sector. Thus the Act should guide practice for all agencies.

While the privacy of individuals must be promoted and protected, there are situations when personal information needs to be shared with other agencies and the Act recognises this. For example, some clients who access services have multiple and complex needs. In order for these needs to be met, clients often require assistance from different sectors such as social services, health and justice. Consequently, multiple agencies, often within the same sector, are often involved with a client, each endeavouring to address a certain need or needs. However, these needs may stem from interrelated causes and in order to improve outcomes for the client, a holistic view which includes all relevant factors is needed.[8] Ascertaining this holistic view requires each agency to share their information or 'piece of the puzzle' about a client so the full picture may be revealed – "[T]he sharing of information and dialogue between the holders of information is a critical, if not the most critical, component of multi-agency and inter-professional liaison and cooperation."[9]

Sarah's Story

Sarah* lives with her partner and her children. Recently her gambling, which had been the occasional scratchie ticket, has reached the level of being addiction and she is spending over $200 per week across a variety of areas. Sarah's addiction is taking its toll on her family, her relationship with her partner is strained and her children have started to misbehave at school. The school contacts Sarah after concerns arise when the children become defiant and start to hit others when they don't get their own way. This is unusual as the children are normally well-behaved. Additionally, the school gets the Social Worker (based there as part of the Social Worker in Schools programme) to conduct a home visit. During the home visit, the Social Worker discovers Sarah's addiction and the impact it is having on the finances and family so makes a referral to addiction and budget services. In order to provide a wraparound service to best support the family, with Sarah's consent, the Social Worker works with her and is able to connect the agencies working with the family and a multi-agency approach ensues with relevant information being freely shared.

*This case study is fictional but draws on real experiences. Any similarity to real persons is purely coincidental.

[5] *Cabinet Manual 2008* at [8.52].
[6] Privacy Act 1993, s 2(1)(a).
[7] "Personal information" means information about an identifiable individual, Privacy Act 1993, s 2(1).
[8] Lips, M., O'Neill, R., & Eppel, E. (2009). Improving information sharing for effective social outcomes.
[9] New Zealand, Children's Action Plan. (2015, November). *Frequently Asked Questions about Information Sharing in the Children's Action Plan*. Retrieved April 30, 2016, from http://childrensactionplan.govt.nz/assets/CAP-Uploads/AISA/FAQs-about-information-sharing-November-2015.pdf

The Ministry of Justice Background Paper on Improving information-sharing, inter-agency co-ordination and case management to address the drivers of crime[10] acknowledges impediments to information sharing may inhibit good outcomes (in terms of social outcomes and offending levels) for clients with complex needs who require a multi-agency approach and that the effectiveness of services can be compromised resulting in clients not having their needs adequately met. Additionally, the importance of sharing personal information has been emphasised when it comes to family violence and child abuse/neglect. As articulated by Right Honourable Sir Anand Satyanand in his role as Advisory Expert Group on Information Security Chair:

> A common theme in child abuse reviews is that vulnerable children could have been protected from harm, if involved professionals had had access to information held elsewhere. We have learned that access to the right information at the right time can make all the difference. There can no longer be any excuse for failing to protect a child if any one of us has information that they are at risk.[11]

A lack of information sharing has been identified as one of the contributing factors in several highly publicised cases of family violence and child abuse/neglect with coroners referencing a lack of information sharing as being a failing.[12] When commenting on one case, Justice Minister Amy Adams stated that "…government officials and those working with children and families are often over-cautious when it comes to sharing information" and that "[t]here is a high level of misunderstanding and almost catatonia about sharing information".[13]

Conversely, erroneous or over-sharing of client information can also be problematic, occasionally leading to significant breaches of clients' rights and the potential for hurt and humiliation of the client. For example, despite the stipulations of the Privacy Act 1993, several significant high-profile privacy breaches have occurred such as that in 2011 when the private details of nearly 7000 Accident Compensation Commission (ACC) clients (including more than 250 clients from ACC's 'sensitive claims unit') were mistakenly sent to a member of the public "because of systemic weaknesses within ACC's culture, systems and processes".[14] Similarly, Child, Youth and Family (CYF) have been in the spotlight for privacy breaches. One instance in 2013 saw a "family's private information passed to a third party",[15] and the recipient attempting to blackmail CYF as a result. In

[10] Ministry of Justice. (2010). Addressing the Drivers of Crime. Background Paper: Improving information-sharing, inter-agency co-ordination and case management to address the drivers of crime (pp. 1-16).
[11] Children's Action Plan. (2016, April 28). Sharing information - Approved Information Sharing Agreement. Retrieved April 30, 2016, from http://childrensactionplan.govt.nz/supporting-childrens-teams/info-sharing/
[12] Trevett, C. (2015, August 5). Adams tackles privacy paralysis: Information-sharing push for cases of domestic violence. *New Zealand Herald.* Retrieved from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11491957
[13] Ibid.
[14] Levy, D. (2012, August 23). Cavalier attitude lead to NZ's biggest privacy breach. *The Dominion Post.* Retrieved from http://www.stuff.co.nz/dominion-post/news/politics/7530166/Cavalier-attitude-lead-to-NZs-biggest-privacy-breach
[15] Small, V. (2013, June 11). CYF blackmailed after privacy breach. *The Dominion Post*. Retrieved from http://www.stuff.co.nz/national/politics/8782552/CYF-blackmailed-after-privacy-breach

another case involving CYF, in 2015, when requesting her own personal information a woman was mistakenly sent highly sensitive information about another person who was unknown to her.[16] Insecure disposal of information has also been highlighted by the media when the sensitive details of 56 people with gambling problems were placed in a public rubbish bin and subsequently acquired by a member of the public.[17] This information included the details of well-known business people and a sports personality.

Confusion around the Act is also apparent as highlighted by an Office of the Privacy Commissioner investigation undertaken between August and October 2015 into information requests by government agencies to private companies from the telecommunications, financial services and utilities industries. While these companies do not fall within the sectors targeted in the present study, some relevant findings may nonetheless be gleaned. One finding was that requests for client information were frequently made without search warrants; instead Principle 11(e) and Principle 11(f) of the Privacy Act 1993 were cited. These subsections concern disclosure being necessary to avoid prejudice to the maintenance of the law by any public sector agency and to lessen a serious threat to public health, public safety or the health of an individual respectively. The agency in receipt of the request is not under a legal obligation to provide the information but may choose whether or not to share it. The investigation found that over one thousand information requests were labelled as being made under the Privacy Act 1993 which is a mischaracterisation as the Act provides grounds for disclosure by agencies but not for requests by law enforcement agencies. When commenting on the investigation, Privacy Commissioner John Edwards said that Principle 11 "…is not a power to obtain information…" but that the intent of the principle is to protect information.

Such a mischaracterisation of the Act can have far-reaching consequences as an agency is only to disclose information if they believe on reasonable grounds that is in accordance with exceptions outlined in Principle 11. Pursuant to section 87 of the Act, if a complaint is made regarding the disclosure of information, the onus is on the agency that released the information to prove that an exception for sharing applied and any consequences will be borne by the agency who disclosed the information (rather than the agency who asked for the information). It would be reasonable to assume that this kind of mischaracterisation is happening in other industries.

Of note is that the report also cites a 2015 Horizon Research public survey in which 78% of respondents thought that a court order should be required before any information is released to a government agency.[18] Additionally, the survey found that if a company was to share the respondent's personal information without a court order, 68% of respondents said they would stop doing business with the company. This indicates the majority of

[16] McLeod, H. (2015, November 14). Invercargill woman slams CYF for privacy breach. *Stuff.co.nz*. Retrieved from http://www.stuff.co.nz/national/74029026/invercargill-woman-slams-cyf-for-privacy-breach.html

[17] El-Gamel, N. (2016, January 8). Problem gamblers' privacy breached when list tossed in footpath bin. *Stuff.co.nz*. Retrieved from http://www.stuff.co.nz/national/75689173/problem-gamblers-privacy-breached-when-list-tossed-in-footpath-bin

[18] Horizon Research Limited. (2015, December 7). Warning to companies: 78% want private data protected. Retrieved April 30, 2016, from https://www.horizonpoll.co.nz/page/422/warning-to-c

people surveyed oppose the sharing of their personal information without a court order yet may be indicative of the wider notion that people value their privacy rights.

Specifically, Principle 11 of the Privacy Act 1993 is concerned with restricting the sharing of personal information and outlines certain limits on the disclosure of such information.[19] Pursuant to this principle, an agency that holds personal information shall not disclose the information unless the agency believes on reasonable grounds —

(a) that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or

(b) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information; or

(c) that the disclosure is to the individual concerned; or

(d) that the disclosure is authorised by the individual concerned; or

(e) that non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(f) that the disclosure of the information is necessary to prevent or lessen a serious threat[20] to—

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(g) that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or

(h) that the information—

(i) is to be used in a form in which the individual concerned is not identified; or

(ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) that the disclosure of the information is in accordance with an authority granted under section 54.[21]

Family violence and child abuse/neglect cases have highlighted that at times the restrictions on information sharing need to be relaxed. Consequently, Part 9A 'Information Sharing' was introduced into the Act in 2013. This addition established a new legal framework, known as Approved Information Sharing Agreements (hereafter AISAs), which

[19] Privacy Act 1993, s 6.

[20] Serious threat is defined in Privacy Act 1993, s 2(1) as a threat that an agency reasonably believes to be a serious threat having regard to all of the following: (a) the likelihood of the threat being realised; and (b) the severity of the consequences if the threat is realised; and (c) the time at which the threat may be realised.

[21] Privacy Act 1993, s 54: Commissioner may authorise collection, use, or disclosure of personal information in special circumstances if certain requirements are met.

provide a mechanism for information sharing that is finely balanced with the competing privacy interests of individuals.

> 96A Purpose of Part
> (1) The purpose of this Part is to enable the sharing of personal information to facilitate the provision of public services.
> (2) To achieve that purpose, this Part—
> (a) provides a mechanism for the approval of information sharing agreements for the sharing of information between or within agencies; and
> (b) authorises exemptions from or modifications to—
> (i) any of the information privacy principles (except principles 6 and 7, which relate respectively to the right to have access to, and correct, personal information):
> (ii) any code of practice (except any code of practice that modifies principles 6 and 7); and
> (c) reduces any uncertainty about whether personal information can be lawfully shared for the provision of the public services, and in the circumstances, described in approved information sharing agreements.

Approved Information Sharing Agreements authorise the parties to share information with each other in accordance with specific terms.[22] At the time of writing this report, three AISAs have been instituted.[23] The Approved Information Sharing Agreement for Improving Public Services for Vulnerable Children is one of these three and "is intended to facilitate information sharing between agencies working collaboratively to identify vulnerable children; protect vulnerable children from harm; and promote the wellbeing of vulnerable children, their families and whanau".[24] Presently, the parties to the three AISAs are government organisations.

Against this background, it becomes clear that agencies can be torn between competing ideals; the requirement and desire to protect the privacy rights of clients and the need to share information in order to increase efficacy and improve outcomes. While AISAs endeavour to facilitate information sharing, it is currently unknown if agencies understand and apply the terms of these agreements in practice.

---

[22] Privacy Act 1993, s 96D.
[23] Supply of adult passport information for the purpose of locating overseas based student loan borrowers and child support liable parents living overseas who are in default of their repayment or contact obligations: Information Sharing Agreement made on 6 June 2014; Information sharing agreement made between Inland Revenue and the New Zealand Police on 2 July 2014 entitled 'Information Sharing Agreement Between Inland Revenue and New Zealand Police relating to disclosure of personal information to New Zealand Police for the purpose of prevention, detection, investigation or providing evidence of serious crime pursuant to Part 9A of the Privacy Act 1993 and section 81A of the Tax Administration Act 1994, July 2014, as amended 16 March 2015'; Approved Information Sharing Agreement for Improving Public Services for Vulnerable Children dated 25 June 2015. Privacy Act 1993, schedule 2A.
[24] Privacy Commissioner. (2015). *Approved information sharing agreement: improving public services for vulnerable children.* A report by the Privacy Commissioner to the Minister of Social Development under section 96P of the Privacy Act 1993.

This report seeks to examine and assess practitioner and organisational competency across a range of agencies relating to the privacy principles with a specific focus on the sharing of personal information pursuant to Principle 11 and Part 9A of the Privacy Act 1993.

METHODOLOGY

Methodist Mission Southern (The Methodist Mission), a multi-disciplinary social service agency that has been operating throughout Dunedin and Otago since 1890, conducted the research. For more information on The Methodist Mission, see Appendix One.

A triangulated mixed-method research design was employed whereby both quantitative and qualitative data were collected concurrently and then analysed in order to elicit rich data and understand the research problem comprehensively.

For the quantitative component, two anonymous online surveys were circulated nationwide canvassing agencies in the following sectors and sub-sectors:

- Social services:
  - Agencies with a high number of social workers
  - Agencies specialising in youth work
  - Counselling services
  - Budget advisory services
  - Anti-violence agencies
  - Parenting/child services providers
  - Specialist Māori providers
  - Specialist Pasifika providers
- Health
  - General practitioners
  - Mental health services providers
  - Disability support providers
  - Aged care facilities
  - District Health Board departments
  - Māori health services providers
- Education
  - Early learning centres
  - Primary schools
  - Secondary schools
  - Tertiary institutes
- Justice and legal
  - Police
  - Corrections
  - Legal services providers
  - Ministry of Justice
- Other government agencies
  - Child, Youth and Family

One of the surveys was directed at practitioners and the other at senior practitioners/managers in order to obtain insight at a practitioner-based and operational level respectively. Respondents were instructed to complete the survey relevant to their role. The surveys were designed to be completed in five to ten minutes. Respondents

were invited to participate via email and were recruited using The Methodist Mission networks and circulation via various databases and well-connected stakeholders. Approximately 4,000 people were invited to participate.

Of the 146 completed survey responses 65 were practitioners and 81 were senior practitioners/managers. Respondents were from both government and non-government organisations. For the practitioner survey, 38% (n=25) of participants were from government organisations and 62% (n=40) were from non-government organisations. For the manager survey, 23% (n=19) of participants were from government organisations and 77% (n=62) were from non-government organisations. Additionally, respondents from the manager survey were recruited from organisations varying in size with the largest group of respondents being from organisations who had 1-20 staff members (including full-time, part-time and volunteer staff members) followed by organisations with more than 100 staff members. Descriptive statistical analysis using Microsoft Excel was used to interpret the data.

For the qualitative component of the study, face-to-face semi-structured interviews were conducted with Otago based participants and phone interviews were conducted with participants located elsewhere in New Zealand. Participants were recruited drawing on The Methodist Mission networks and snowball (chain-referral) sampling. In total, 20 interviews were conducted, 10 with senior practitioners/managers and 10 with practitioners. Thematic coding (a method which identifies, analyses and reports patterns/themes within data) was employed to examine the data acquired.

The wide range of organisations targeted for both components of this project enabled analysis of cross-sector information sharing relationships and comparative analysis of practitioner and organisational competencies in addition to the structural and operational factors present. Furthermore, a broad range of target organisations enabled comprehensive recommendations and practical resources to be created that address major shortcomings and challenges in relation to the principles and information sharing in practice.

RESULTS AND FINDINGS PART ONE

Training on the Privacy Act and privacy principles

In light of the Act's all-inclusive application it was anticipated that all participants would be trained in the principles. In the practitioner survey, respondents were asked if they had received training/instruction from their current employer on how to use the principles of the Act in their practice. While the majority of respondents (68%)[25] answered that they have received training/instruction on using the principles, nearly one in three respondents (32%) answered that they have not. This conflicted somewhat with the organisational level survey. For that survey, 79% of respondents answered that their staff members who have access to client information receive training/instruction on how to use the principles of the Act in their practice while 17% said their staff do not and 4% said they do not know.[26] While the surveys were anonymous and therefore response cannot be matched, this conflict is concerning given the potential for breaches of the principles and the need to protect both clients and organisations.

Of those respondents who had received training/instruction, over half (59%) reported they had received training in the last year and 34% said they had received training over a year ago. A small number (7%) of participants said they had received training within the last month with no respondents answering that they have been trained in the last week (see Figure 1).

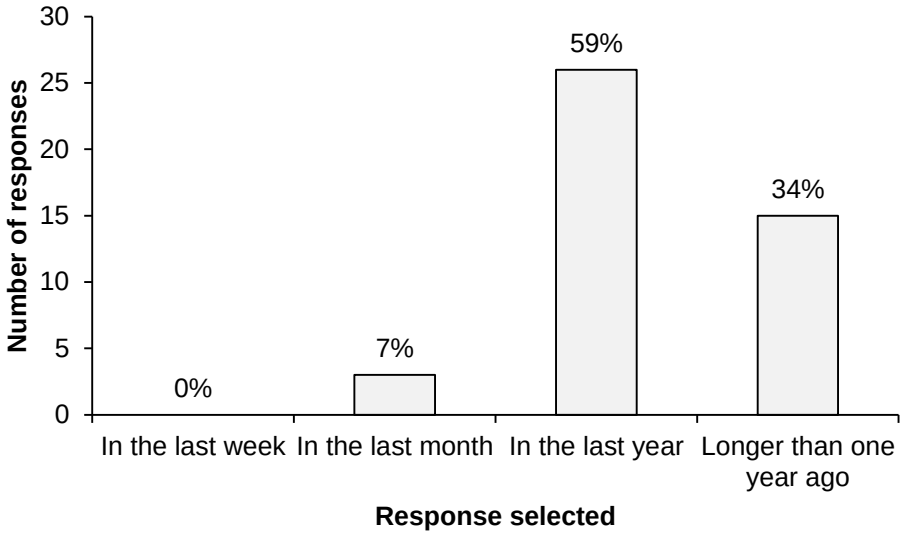

Figure 1. Responses selected for the question: When did you last receive training/instruction from your current employer on how to use the Privacy Act 1993 in your practice? *N* = 44

[25] Note: For ease of reading, percentages have been rounded to the nearest whole number. In some instances, this may mean that in total the percentages do not add to exactly 100%.
[26] This discrepancy may be due (in part) to the differing number of participants in each survey.

As shown in Figure 2, when asked to select what their training consisted of, 70% of the responses were that this training involved being given information about the Act to read, followed closely by discussion in a team setting of the principles and how they are applied (66%). Thirty-nine percent of the responses were that their manager/team leader has explained the principles to them while a small number (5%) of the responses were that they had received training/instruction in a different form.

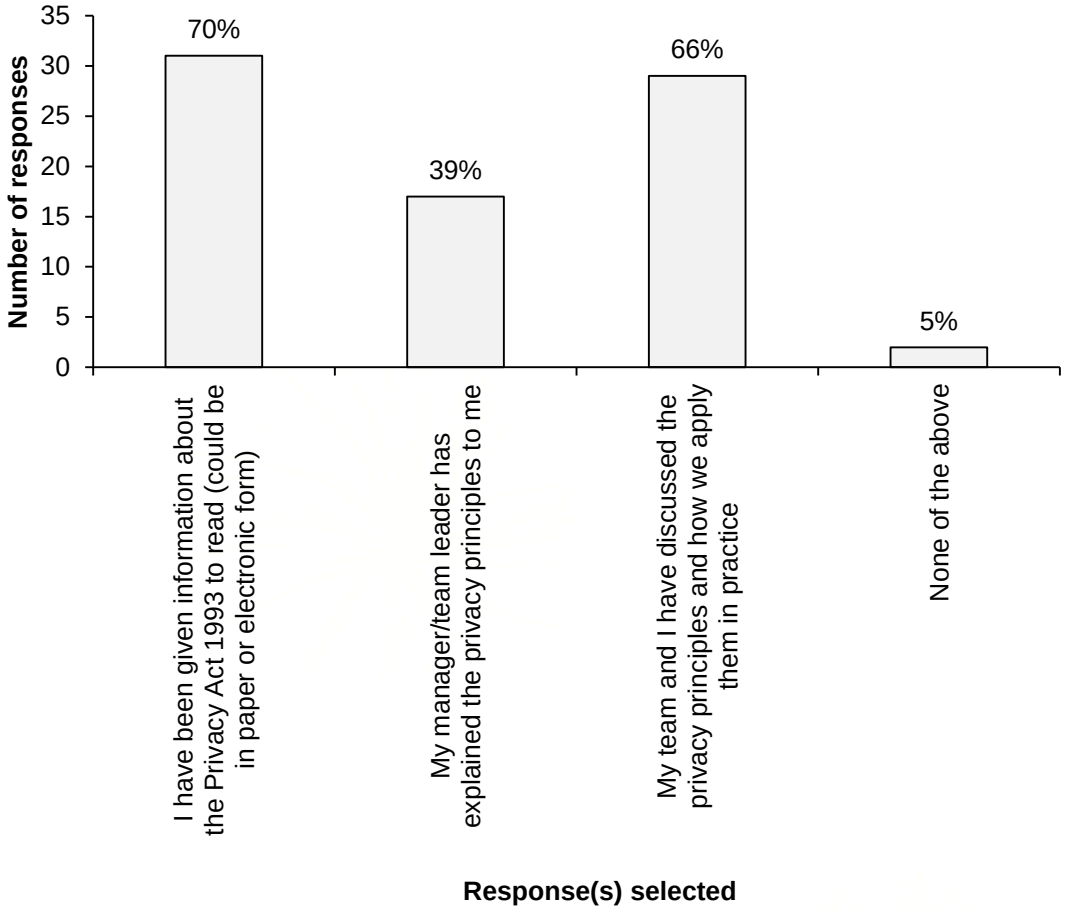

Figure 2. Responses selected for the question: Thinking about your training/instruction, which of the following apply to you? (Select all that apply). *N* = 44

The organisational level survey recorded that the majority of training is being conducted in-house, with only 31% responding that they provide external training and 36% reporting that training is provided as the need arises (Figure 3). Respondents were also given the opportunity to specify if there was another way training takes place. Responses included "online evidence based learning" and having the practitioner take responsibility for their knowledge of the Act: "Staff must read and be aware of the Privacy Act as it relates to their working relationship" (for the complete list of specified responses see Appendix Three and Appendix Four). The majority (61%) of practitioners responded that they are trained less than annually while 23% said they are trained annually and 16% said they are trained more frequently than once a year (Figure 4).

Responses were mixed when respondents were asked how easy or difficult it is to apply the principles in their practice. As seen in Figure 5, only 12% of respondents said applying the principles was easy and 25% somewhat easy. Forty percent of respondents said it was neither easy nor difficult while 11% found it somewhat difficult and 5% difficult. It is disconcerting that 8% of respondents reported that they did not know the principles. One of the reasons for this may be inadequate training.

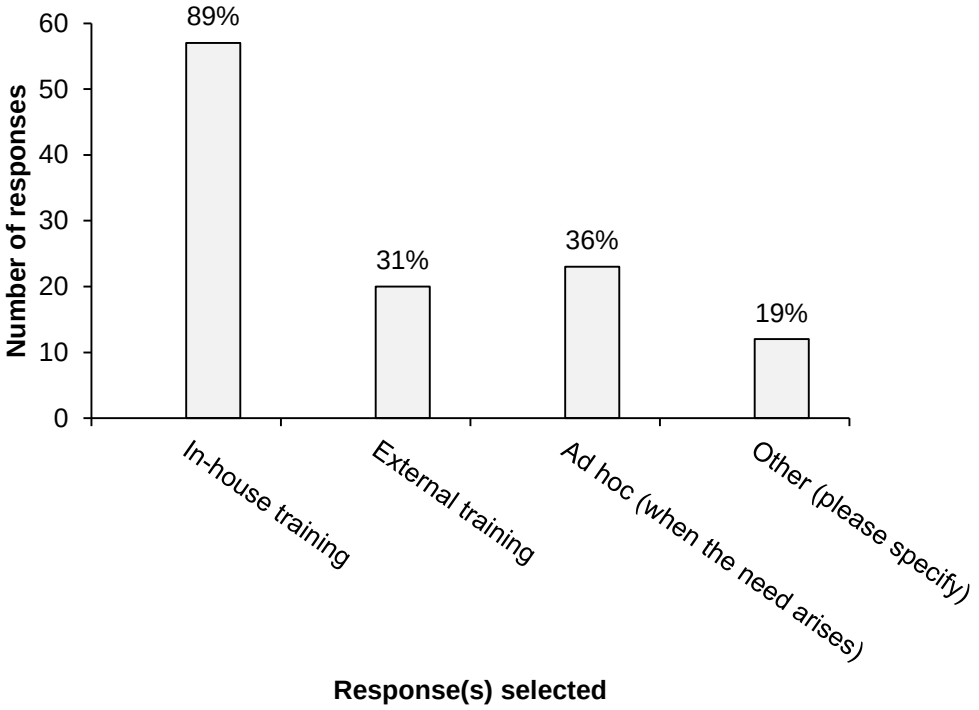

Figure 3. Responses selected for the question: How does this training [on how to use the principles of the Privacy Act 1993 in practice] take place? (Select all that apply). *N* = 64

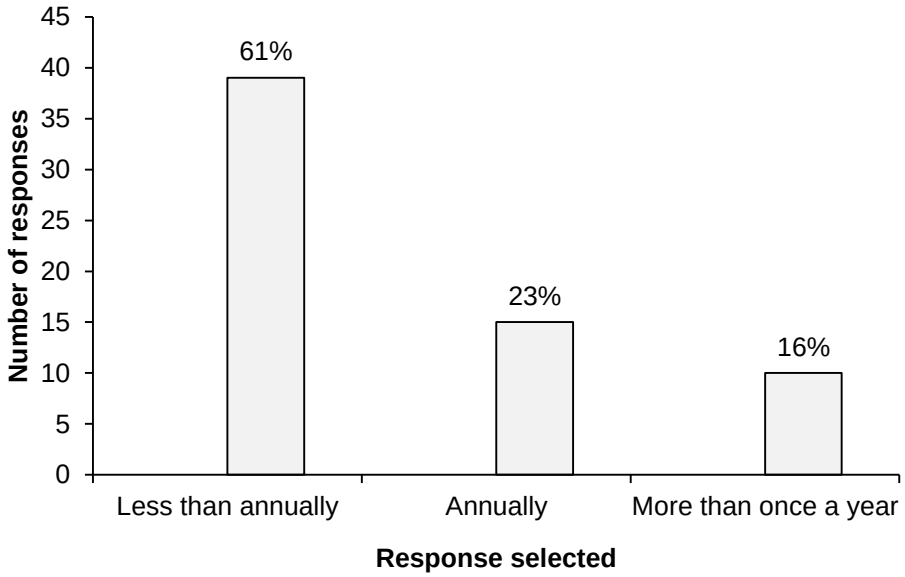

Figure 4. Responses selected for the question: How often does this training take place? *N* = 64

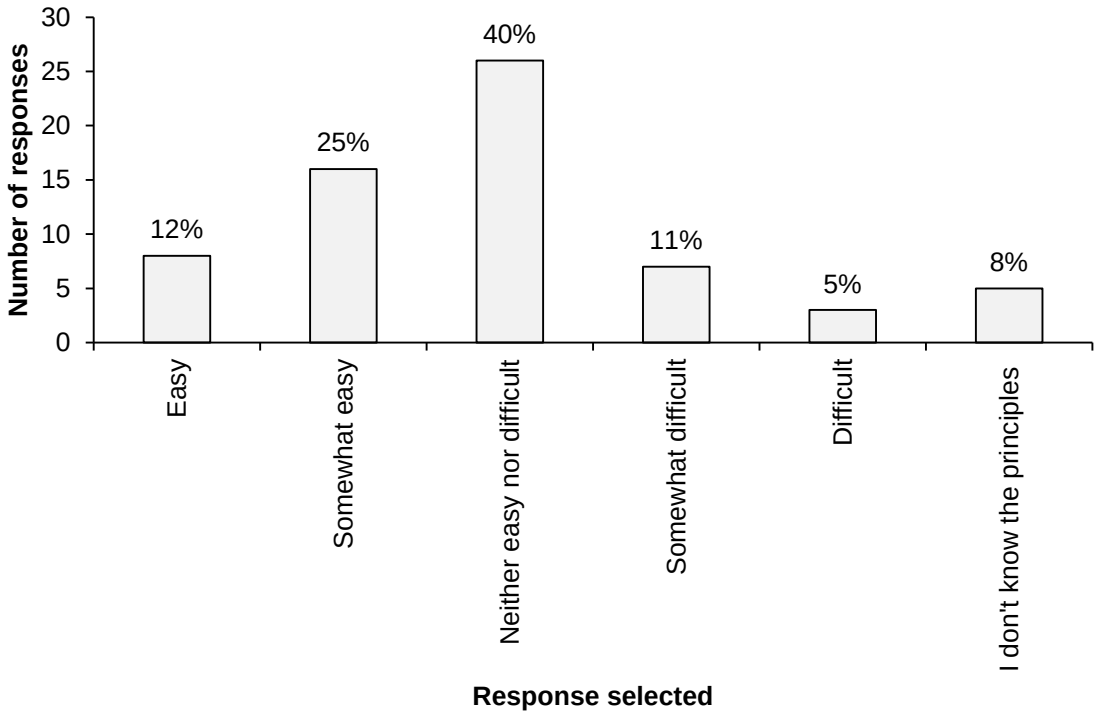

Figure 5. Responses selected for the question: Please indicate your response to the following statement: "Applying the Privacy Act 1993 principles in my practice is:" *N* = 65

When asked if their organisation is providing training/instruction to staff members on when another Act or formal Memorandum of Understanding may apply that concerns sharing client information, less than 60% of respondents answered that they do (Figure 6). This is especially concerning given that the Act is subject to all other legislation and therefore

obligations of sharing and withholding information may be different to those outlined in the principles.

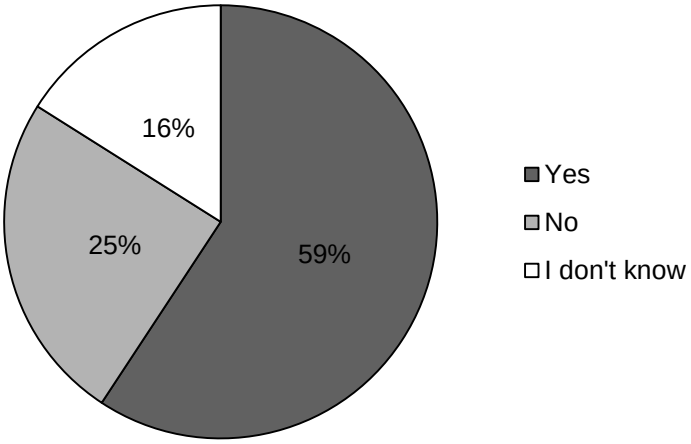

Figure 6. Responses selected for the question: Do staff members receive training/instruction on when another Act (law) or formal Memorandum of Understanding may apply that concerns sharing client information? *N* = 81

Information handling policies and privacy officers

Ninety-five percent of respondents in the organisational level survey responded that their organisation has an information-handling policy[27] while 2% responded that their organisation does not have one and 2% said they do not know. Ninety-nine percent of those who answered that they do have such a policy said that staff are given access to this policy (1% said they do not know if staff are given access).

A concerning trend and example of non-compliance with the Act emerged when examining the results of the survey questions surrounding privacy officers. The majority of respondents (55%) said that they do not know who the privacy officer at their organisation is (Figure 7). For the organisational level survey, 56% of respondents answered that their organisation has a designated privacy officer while 35% said their organisation does not (Figure 8). Pursuant to section 23 of the Act, each agency must have at least one privacy officer who is tasked with (inter alia) encouraging and ensuring compliance with privacy principles and dealing with requests made to the agency under the provisions of the Act. It should be noted that some organisations may not use the term 'privacy officer' specifically or may assume that this would be the designated person's only role within the organisation. To mitigate the effect of this on the results, the following explanatory statement was provided with this question: "*The person at your organisation who is responsible for ensuring compliance with the Privacy Act 1993, training staff in privacy matters as well as handling requests for, and general issues about, personal information. Note that this may not be their only job function but may be integrated into a person's existing role." Importantly, for those organisations without a designated privacy officer, it

[27] Whether this be a stand-alone policy or a statement/protocol/procedure contained within a broader policy.

may be difficult for staff to obtain advice or if they were to seek advice from someone not sufficiently trained in the Act incorrect information may be given.

Sixty percent of the respondents who said their organisation had a privacy officer responded that they make staff aware of who the privacy officer is while 16% said they do not (Figure 9). Of those organisations who said they do make staff aware of who the privacy officer is, 78% responded that they do so during induction, 37% do so during staff training and 30% when the need arises (Figure 10). It is possible that staff who are only made aware of the privacy officer as part of their induction may forget this information and this may explain the lack of awareness regarding the privacy officer.

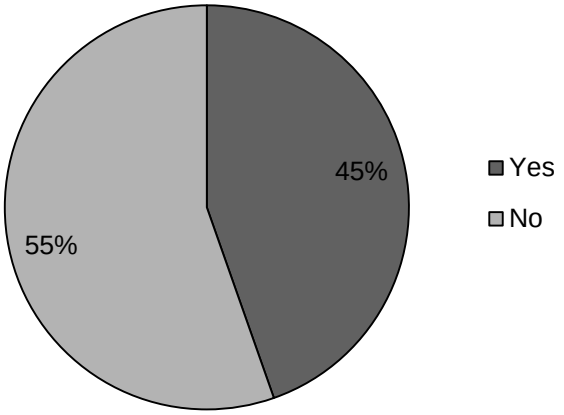

Figure 7. Responses selected for the question: Do you know who the Privacy Officer* at your organisation is? *N* = 65

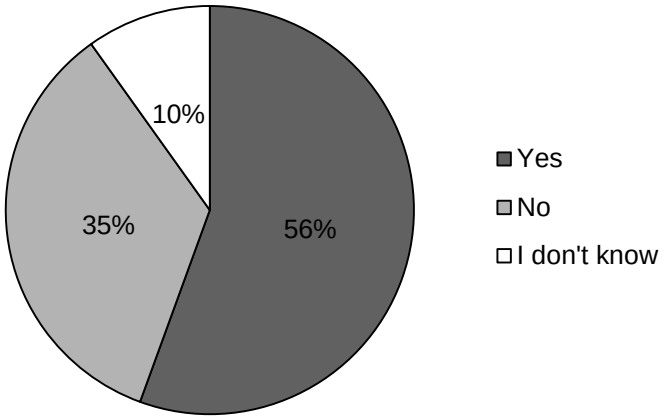

Figure 8. Responses selected for the question: Does your organisation have a designated Privacy Officer*? *N* = 81

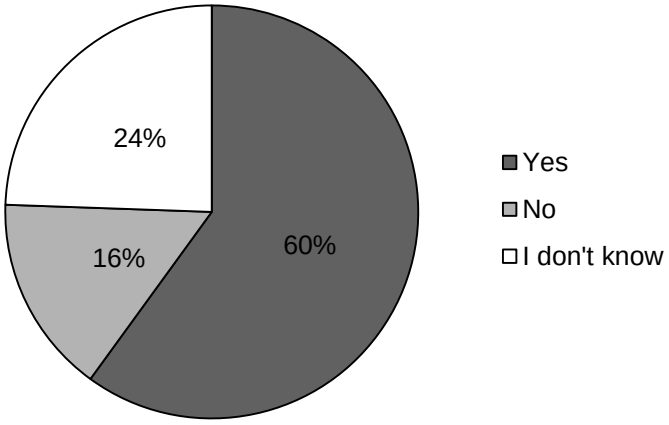

Figure 9. Responses selected for the question: Are all staff members made aware of who the Privacy Officer is? *N* = 45

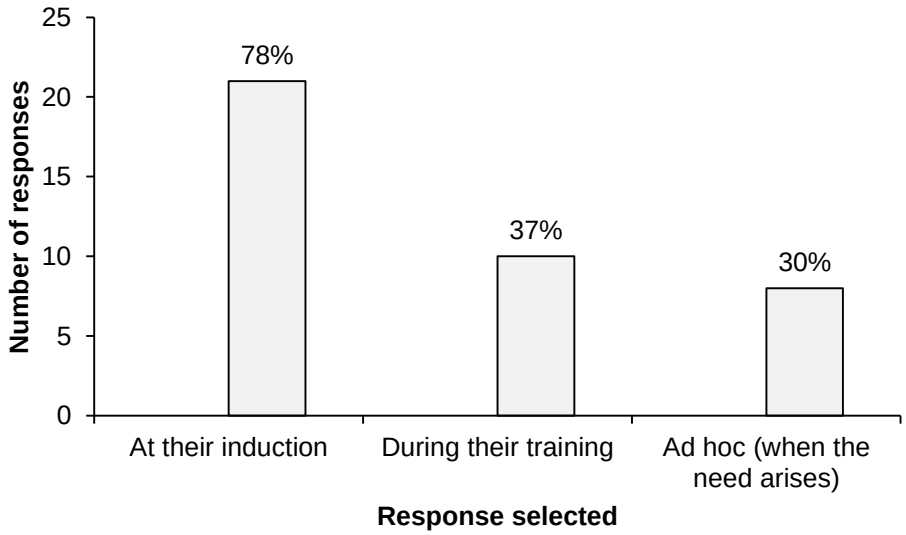

Figure 10. Responses selected for the question: When is a staff member made aware of who the Privacy Officer is? (Select all that apply). *N* = 27

Only twenty-nine percent of respondents answered that their privacy officer had undergone training administered by the Privacy Commissioner (Figure 11). This was surprising as this training is free, can be done online at any time and would help ensure that privacy officers have the knowledge and skills to undertake their role.

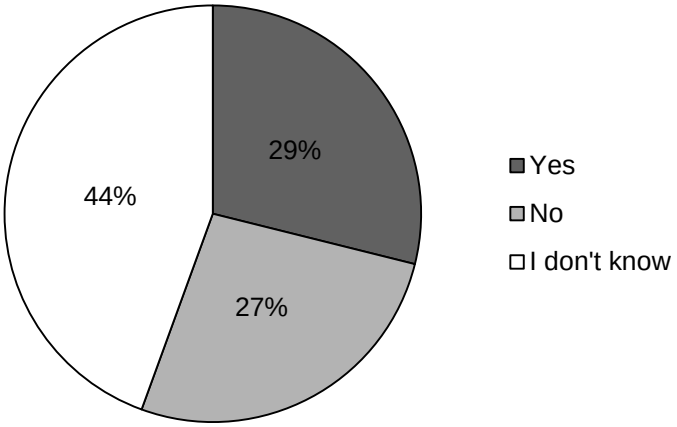

Figure 11. Responses selected for the question: Has the Privacy Officer undergone training administered by the Privacy Commissioner? *N* = 45

Collecting personal information from a client

As seen in Figure 12, only 68% of practitioner respondents said they almost always explain to the client the purpose of why they are collecting a client's personal information while 20% said they do so often.[28] In most cases this explanation is given verbally (96%), largely in conjunction with a written explanation (80%) (Figure 13). Pursuant to privacy Principle 3: *Collection of information from subject*, when an agency collects personal information from an individual, they must take reasonable steps in the circumstances to ensure that the individual is aware of (inter alia) the fact that the information is being collected. However, these survey results would suggest that not all practitioners are complying with this principle on every occasion.[29] These results conflicted with those of the organisational level survey where 89% of respondents said that their organisation requires staff to explain the purpose of collection to the client (Figure 14).

For the most part, practitioners considered themselves to be very confident or confident when it comes to identifying the circumstances in which they are permitted to collect a client's personal information (Figure 15).

[28] To avoid confusion an explanation as to what is meant by collection was provided: *Please note that 'collecting' refers to when you ask for information from a client and does not include the receiving of unsolicited information that the client volunteers.
[29] Of note: some limited exceptions to this requirement are outlined in Principle 3.

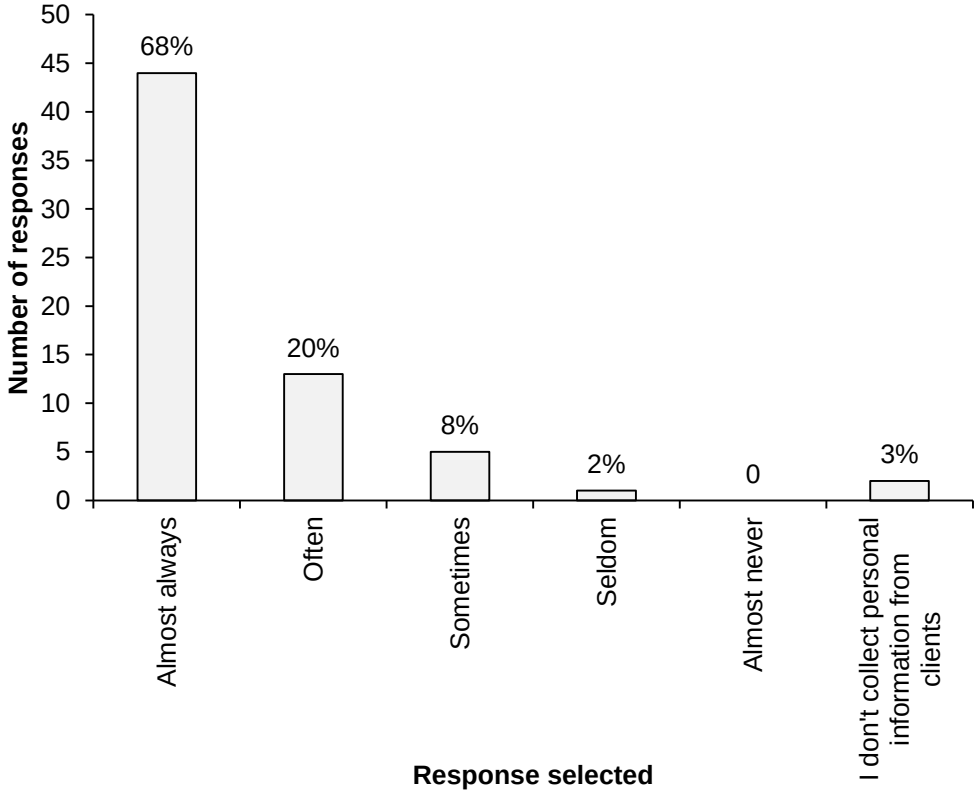

Figure 12. Responses selected for the question: When collecting* personal information from a client, how often do you explain to the client the purpose of why you are obtaining that information? *N* = 65

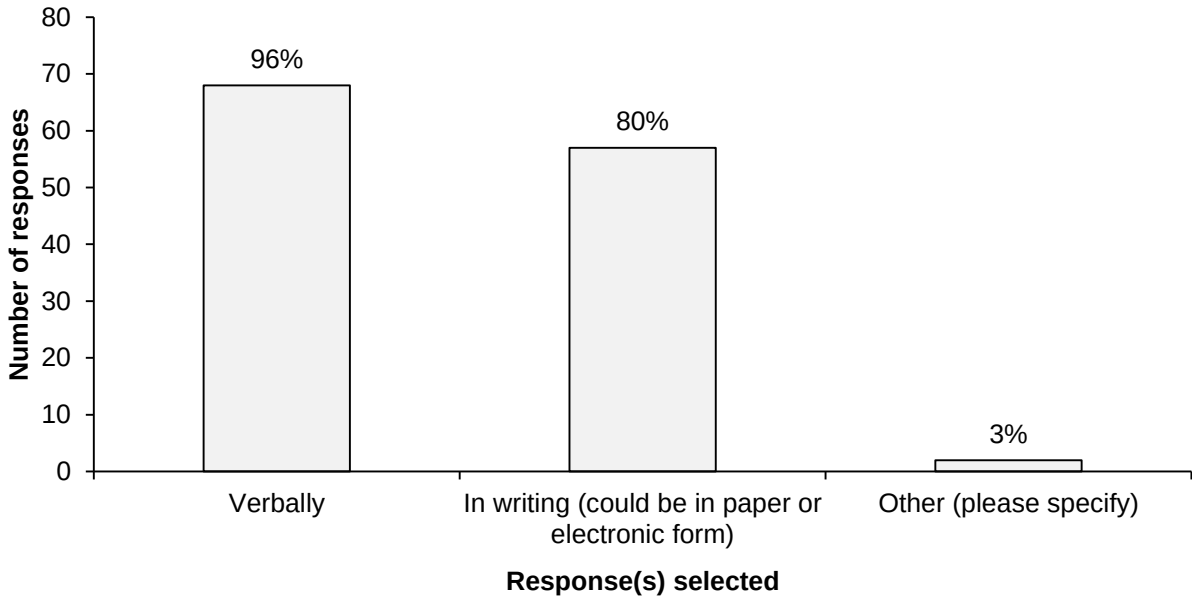

Figure 13. Responses selected for the question: How is this explanation conveyed to the client? (Select all that apply). *N* = 81

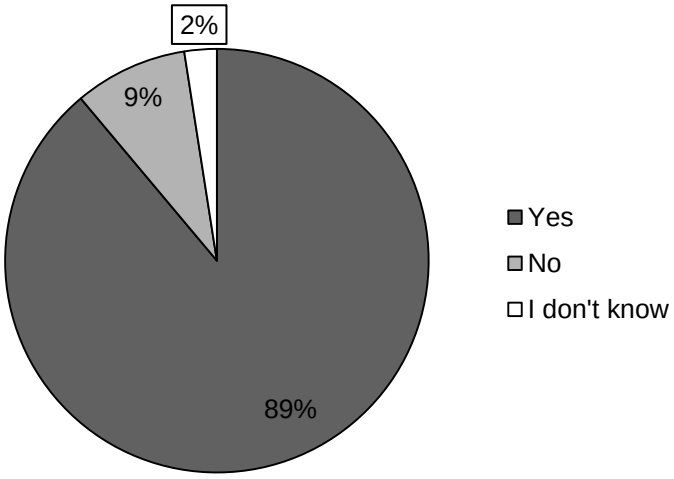

Figure 14. Responses selected for the question: Does your organisation require staff to explain to clients for what purpose they are collecting the client's information and how this will be used and stored? *N* = 81

As seen in Figure 16, when collecting information from a client, most respondents said they were confident (42%) or very confident (43%) when it came to identifying what they are obligated to tell the client about how the information will be used and stored. Twelve-percent indicated they were neither confident or unconfident while 2% said they were not at all confident.

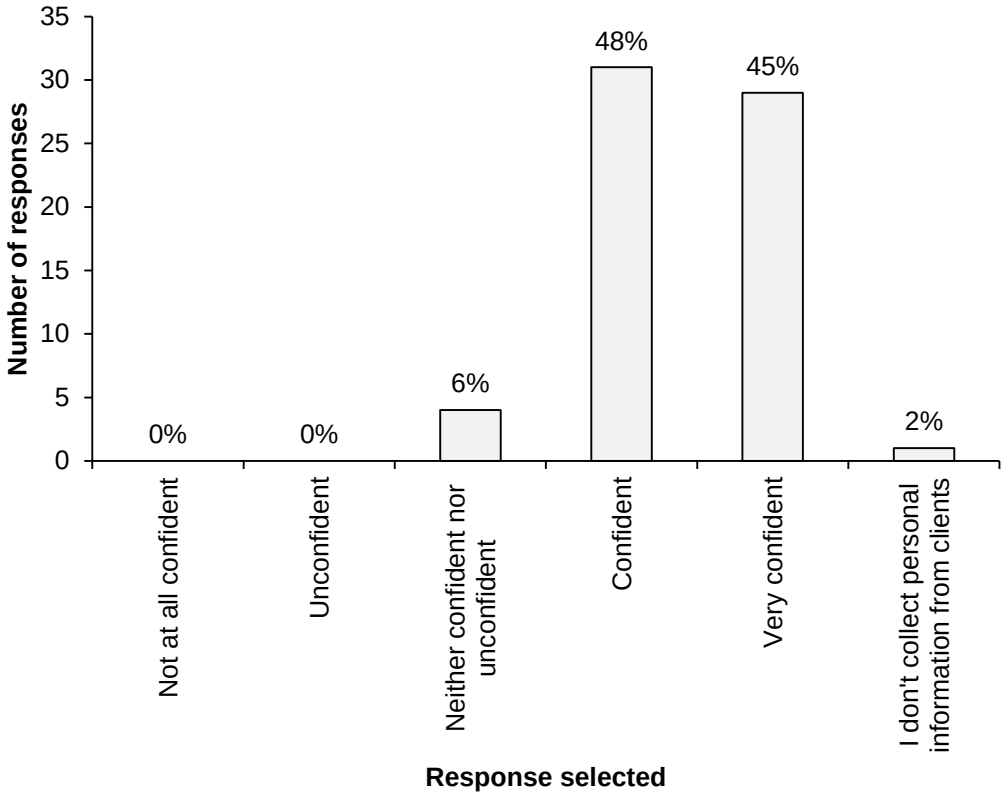

Figure 15. Responses selected for the question: How confident or unconfident are you in identifying the circumstances in which you are permitted to collect a client's personal information? *N* = 65

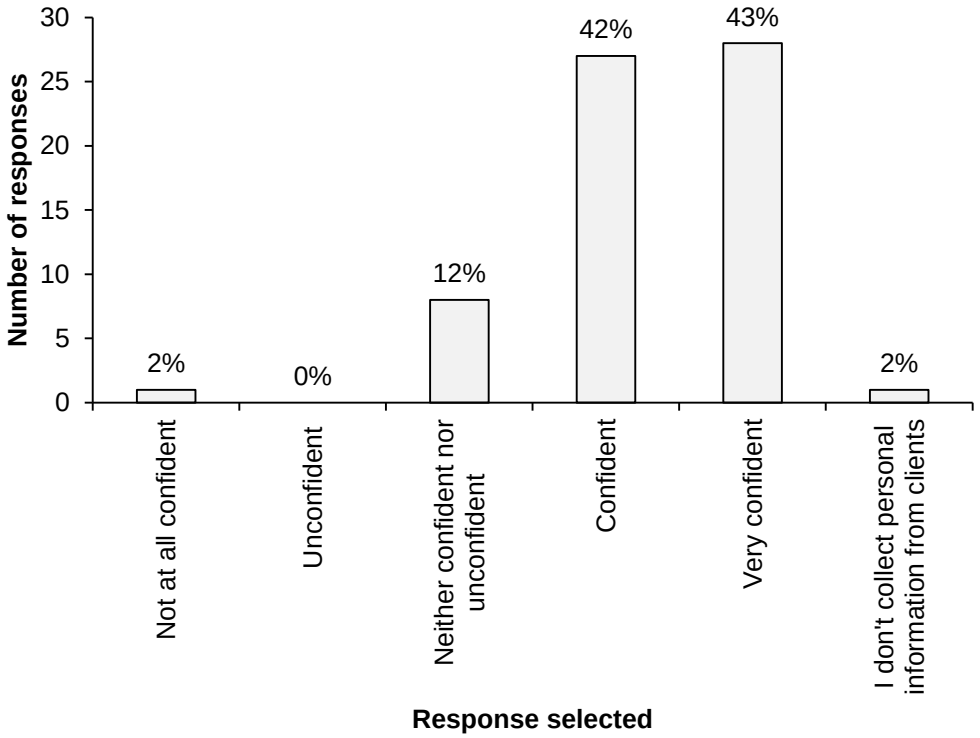

Figure 16. Responses selected for the question: When you collect client information, how confident or unconfident are you in identifying what you are obligated to tell the client about how the information will be used and stored? *N* = 65

Seventy-nine percent of manager respondents said their organisation have a policy about what kind of information staff may collect from clients while 17% said their organisation does not and 4% of respondents said they do not know. This is of concern as Principle 1: *Purpose of collection of personal information*, makes clear that information is only to be collected for lawful purposes and the information is necessary for those purposes.

Ninety-eight percent of manager respondents said that their organisation have a policy about how client information is stored and this is therefore likely to assist in complying with the obligations to protect personal information as outlined in Principle 5: *Storage and security of personal information*. Eighty-six percent of manager respondents answered that their organisation has a policy about what happens to a client's personal information when it is no longer required while 10% do not have such a policy. Principle 9*: Agency not to keep personal information for longer than necessary* of the Act requires that personal information is not kept for longer than is required and therefore agencies need a policy needs detailing how and when this information is safely destroyed.

Manager respondents were also asked whether their organisation has ever conducted an audit of its IT security of client information (Figure 17). More than half (56%) either answered that their organisation has not conducted an audit of IT security of client information (23%) or that they do not know whether such an audit has been conducted (33%). While the Act does not make such audits mandatory nor references them

specifically, this could come within the ambit of an agency's obligations under Principle 5: *Storage and security of personal information*. Principle 5 requires that an agency holding personal information ensure that the information is protected by reasonable security safeguards against loss, access, use, modification, or disclosure and other misuse. In the latest PwC Global State of Information Security® Survey 2016 (a New Zealand context),[30] cyber-attacks were described as the "new normal" thus when it comes to keeping personal information safe and fulfilling the requirements outlined in Principle 5, conducting audits of IT security of client information in order to ensure security of electronic data is necessary. Of those who had conducted such an audit, most respondents (64%) indicated that this has been done in the last year (Figure 18).

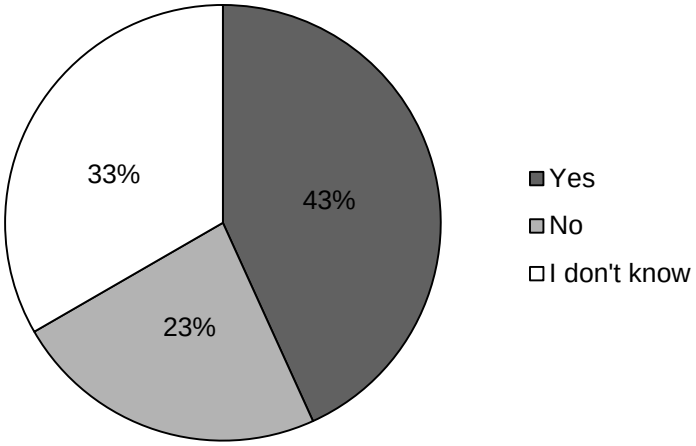

Figure 17. Responses selected for the question: Has your organisation ever conducted an audit of its IT security of client information? *N* = 81

[30] PricewaterhouseCoopers New Zealand. (2016). *Exploring the big cyber questions A New Zealand context: Global State of Information Security Survey 2016*. Retrieved 22 April, 2016, from http://www.pwc.co.nz/PWC.NZ/media/pdf-documents/pwc-security/pwc-global-state-of-information-security-survey-2016-exploring-the-big-cyber-questions-new-zealand-context.pdf

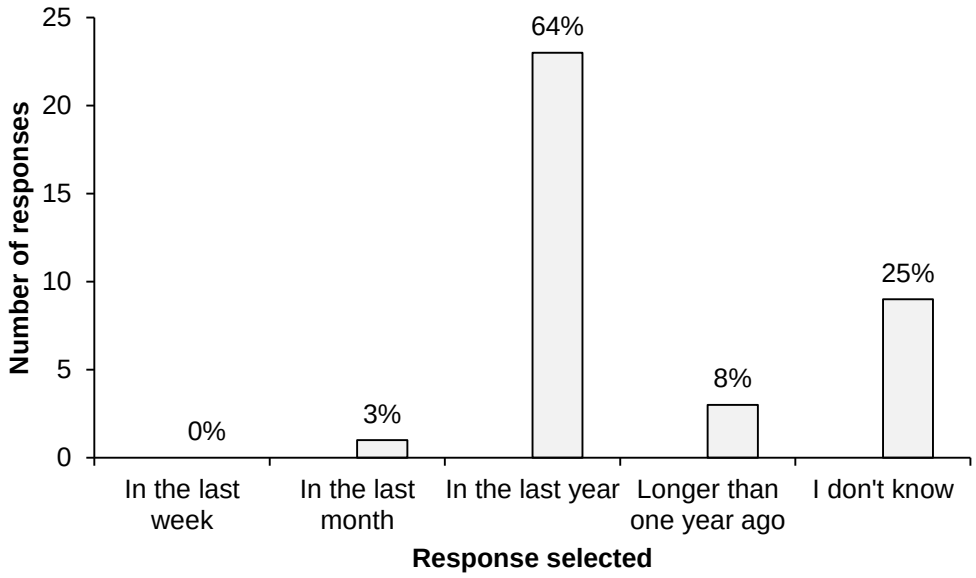

Figure 18. Responses selected for the question: When did the audit last take place? *N* = 36

Access and correction of information at the client's request

Fifteen percent of practitioner respondents considered themselves very confident regarding when they are able to give a client their own personal information and 63% considered themselves confident (Figure 19). Fifteen percent said they were neither confident or unconfident while the remaining 6% considered themselves unconfident. Interestingly, when respondents were asked to rate their confidence when it came to identifying the circumstances in which they can withhold a client's requested personal information, the responses differed markedly. As shown in Figure 20, 11% considered themselves to be very confident and 45% considered themselves to be confident while nearly half (45%) did not consider themselves to be confident with 25% neither confident nor unconfident, 18% unconfident and 2% not at all confident. These results are concerning given the stipulations of Principle 6: *Access to personal information* and the provisions of Part 4: *Good reasons for refusing access to personal information* and Part 5*: Procedural provisions relating to access to and correction of personal information* of the Act. Respondents were also not confident when it came to knowing what time frame they were required to act on personal information requests with 11% responding they were very confident and 29% that they were confident. However, the majority of respondents did not consider themselves to be confident with nearly a third (32%) of respondents answering that they were neither confident nor unconfident, a quarter (25%) unconfident and 3% not at all confident (Figure 21). This suggests a lack of knowledge given that the timeframe is stated in section 40 of the Act.

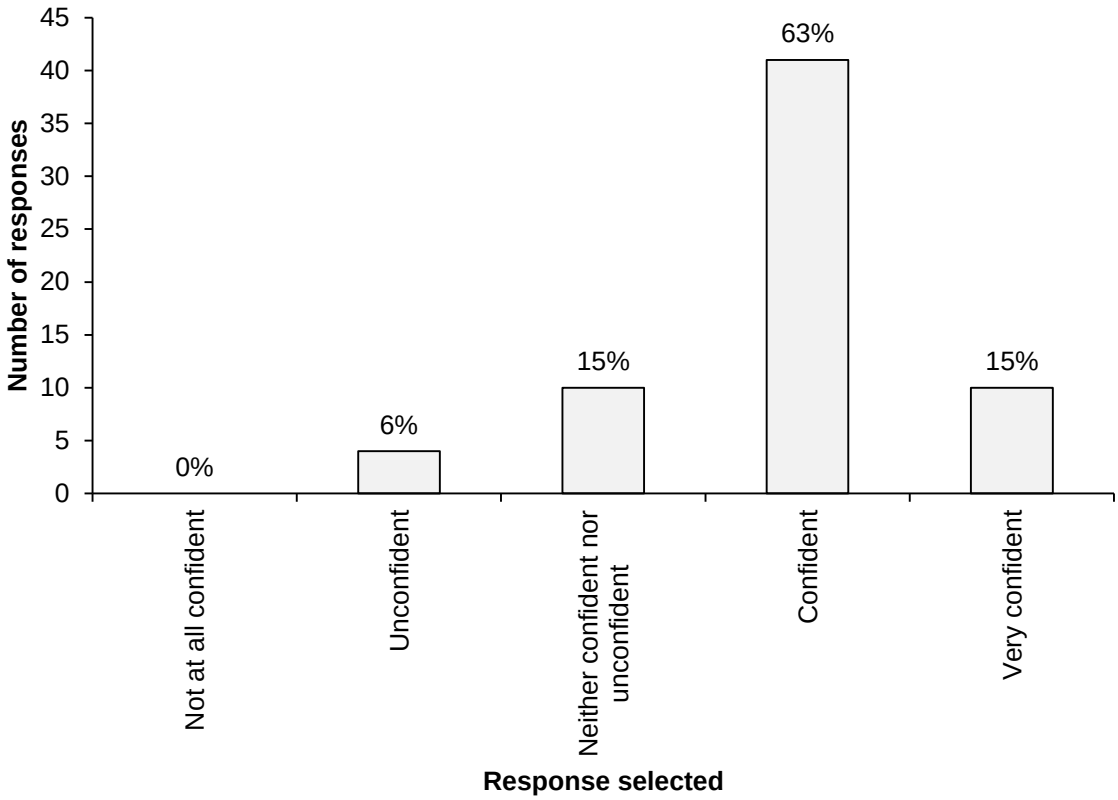

Figure 19. Responses to the question: If a client asks you for access to their own personal information, how confident or unconfident are you in identifying the circumstances in which you can give them that information?

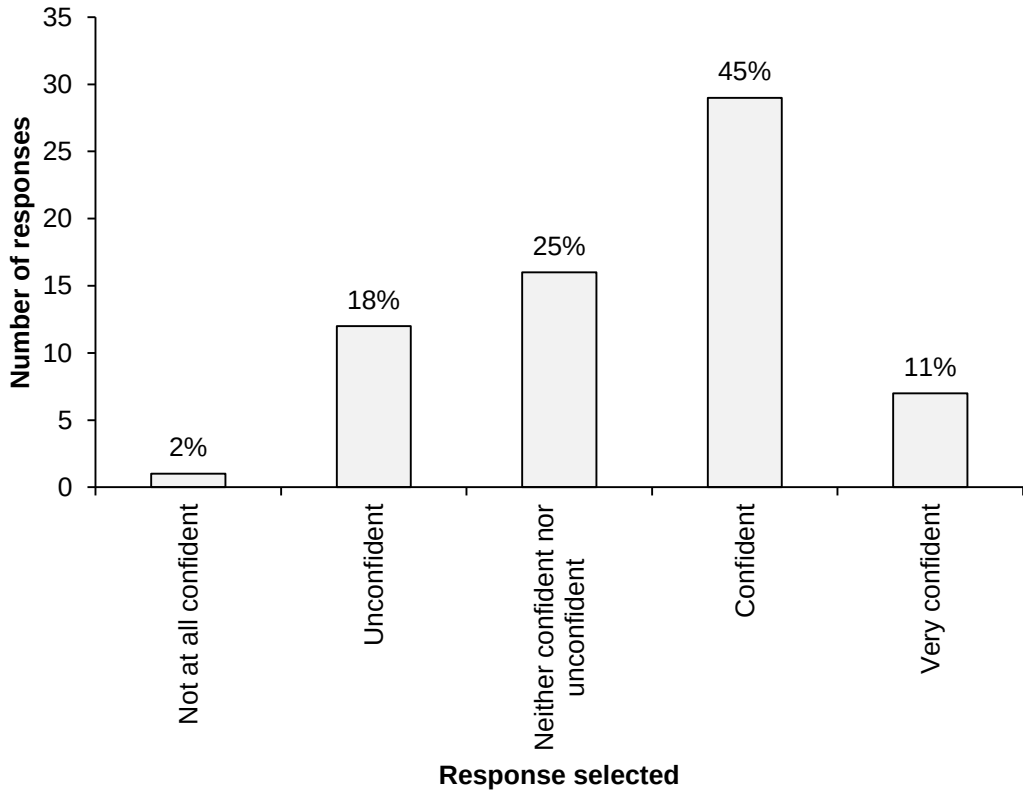

Figure 20. Responses selected for the question: If a client asks you for access to their personal information, how confident or unconfident are you in identifying the circumstances in which you are able to withhold information? *N* = 65

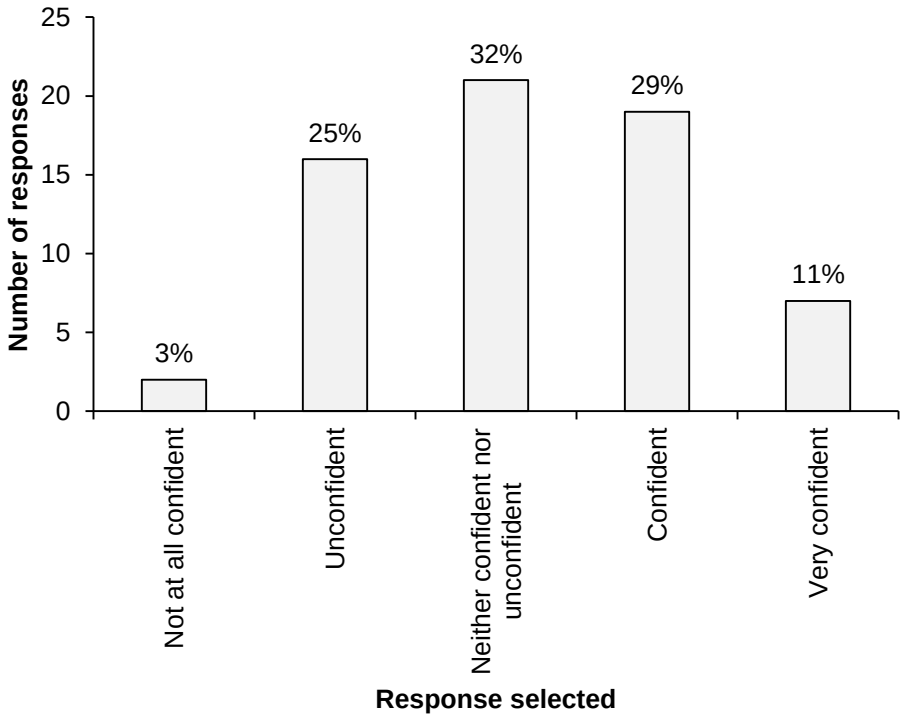

Figure 21. Responses to the question: If a client requests their personal information, how confident or unconfident are you in knowing what time frame you have to act on that request? *N* = 65

Figure 22 shows that 57% of respondents said they were confident in knowing what to do should a client wish to correct their personal information while 20% considered themselves to be very confident. However, this meant that nearly one in four (23%) respondents considered themselves not confident if faced with this situation. This is concerning given Principle 7: *Correction of personal information*, which states reasonable steps must be taken to correct information if requested by the individual or if the agency is unwilling to correct the information, and the individual requests, a note of the request for correction should be attached to the client's information.

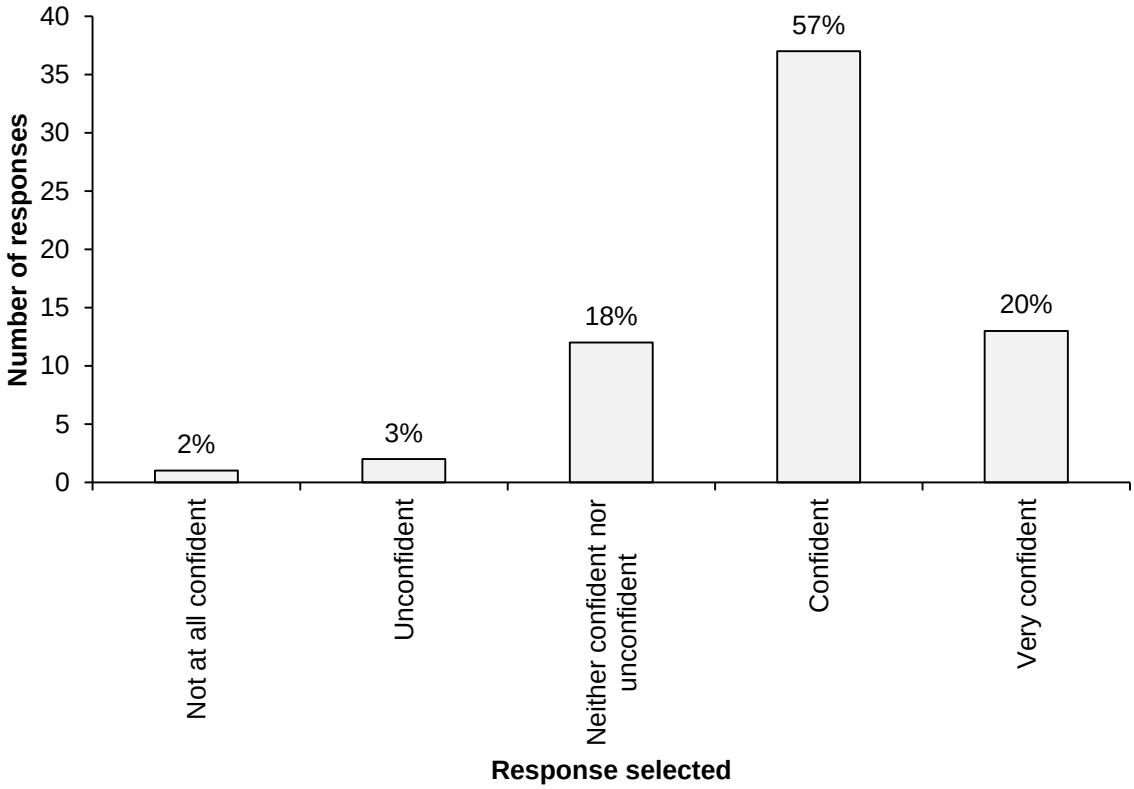

Figure 22. Responses selected for the question: How confident or unconfident are you in knowing what to do should a client wish to correct their personal information held by your organisation? *N* = 65

Sharing client information with other agencies and client consent

As indicated in Figure 23, respondents are engaging in information sharing with nearly 90% of respondents answering that they have shared information with another organisation within the last 12 months with more than a third of respondents answering that they have done so 21 times or more. Results differed somewhat when respondents were asked how many times in the last 12 months they had personally requested information from another organisation (Figure 24). Eighteen percent said they had not made any requests for information while nearly a third (32%) said they had only made between one and five requests. However, nearly a quarter (23%) said they had made 21 or more requests. The results from the organisational level survey had 79% of respondents answering that their organisation receives requests for client information (Figure 25). As seen in Figure 26, of those organisations who do receive requests for client information, most respondents (91%) answered that these requests have been from the client themselves and government agencies (75%). Nearly half (48%) answered that they had received requests from non-government agencies. Twenty-three percent of respondents said they had also received requests from 'other' organisations. Most

respondents specified that these requests came from lawyers and several also mentioned requests being made by family members.[31]

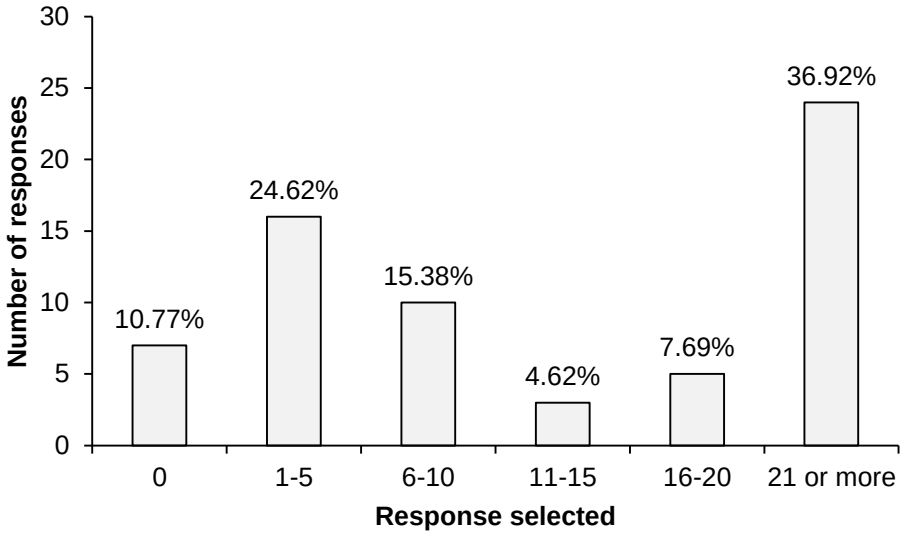

Figure 23. Responses selected for the question: Approximately how many times in the last 12 months have you personally shared information with another organisation? *N* = 65

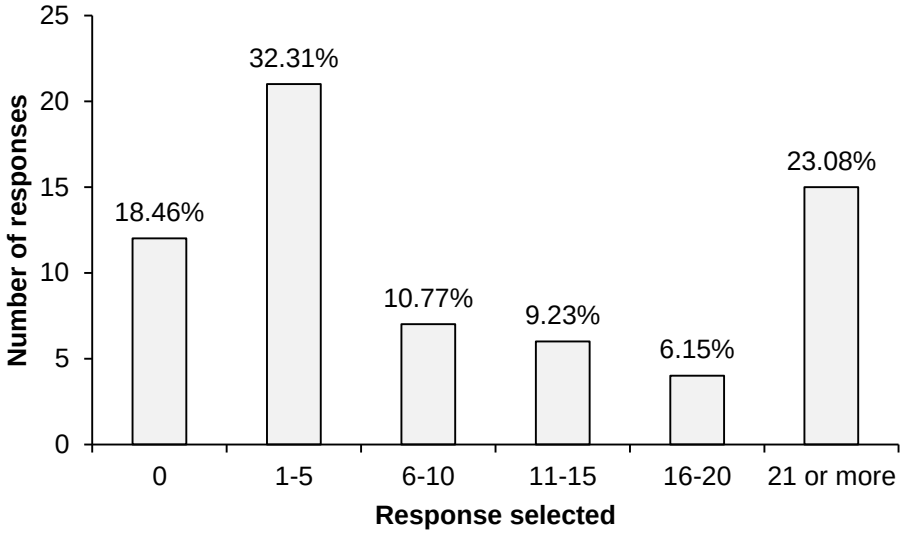

Figure 24. Responses to the question: Approximately how many times in the last 12 months have you personally requested client information from another organisation? *N* = 65

[31] For the complete list of specified responses see Appendix Three and Appendix Four.

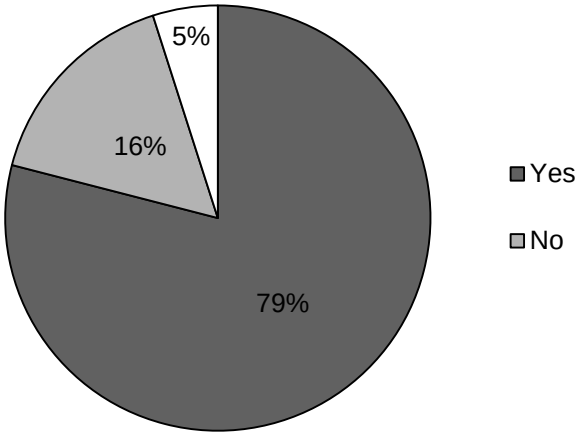

Figure 25. Responses to the question: Does your organisation receive requests for client information?

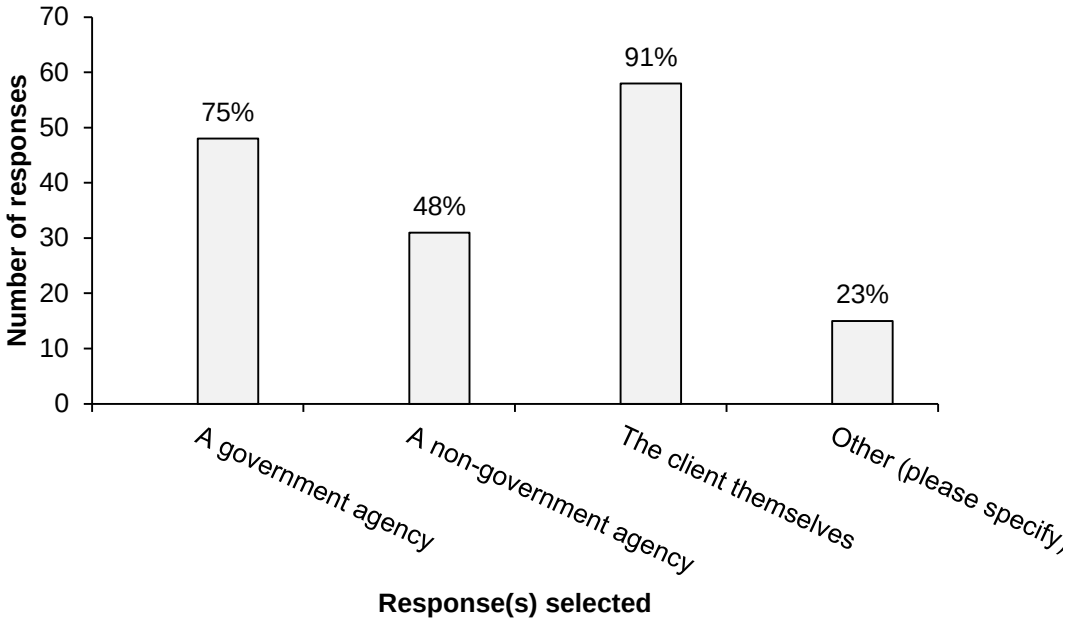

Figure 26. Responses selected for the question: Who has your organisation had requests for client information from? (Select all that apply). *N* = 64

As seen in Figure 27, 17% of respondents considered themselves to be very confident in knowing when the Act permits them to disclose a client's personal information while 52% of respondents considered themselves confident. Nearly one third (32%) of respondents in total did not consider themselves confident in this area. This is surprising as the Act stipulates in Principle 11: *Limits on disclosure of personal information*, that information is not to be disclosed unless it is believed on reasonable grounds that one of the exceptions listed applies. One of the exceptions is getting the client's consent to share the information. When asked whether they knew the circumstances in which they needed to get a client's consent prior to sharing the client's information, 54% responded that they are

very confident and 31% that they are confident with 16% in total indicating they are not confident (Figure 28). This difference and inconsistency between responses to each question elucidates either a potential misunderstanding of Principle 11 or a lack of knowledge regarding disclosure of client information.

Respondents were also asked for their views on gaining the client's consent to share information even in instances when the Act permits them to share this information without consent. Results were fairly evenly split with over one third indicating some level of agreement (36%), nearly one third neither agreeing nor disagreeing (31%) and the remaining third indicating a level of disagreement (34%) (Figure 29).

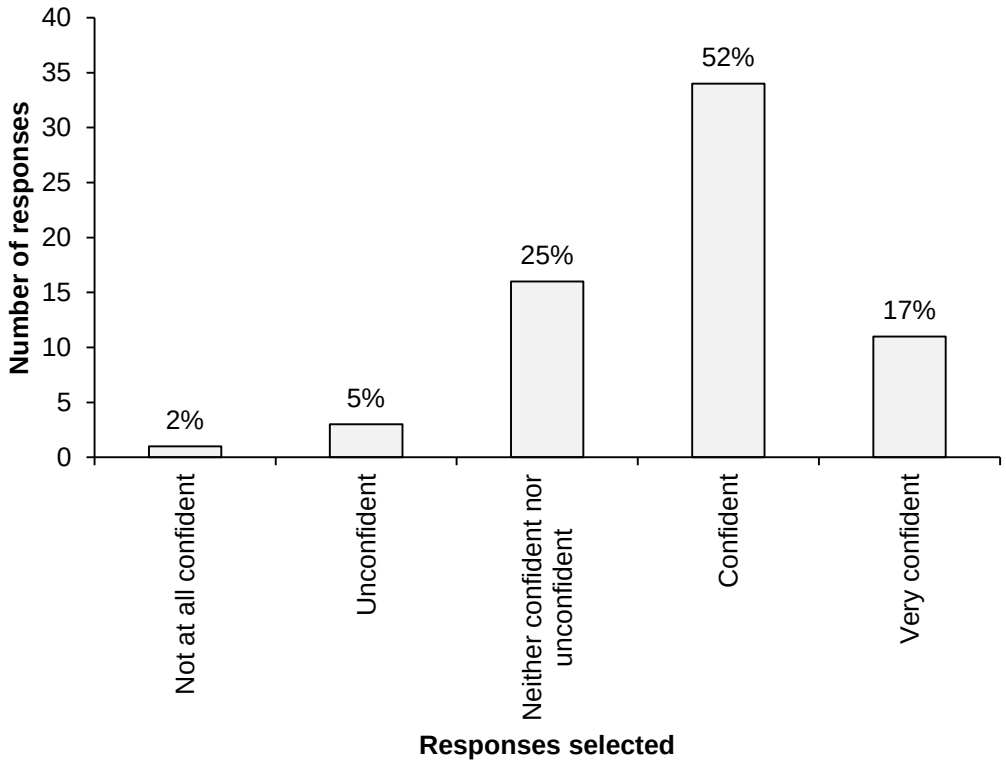

Figure 27. Responses to the question: How confident or unconfident are you in knowing when the Privacy Act 1993 permits you to disclose a client's personal information to others? *N* = 65

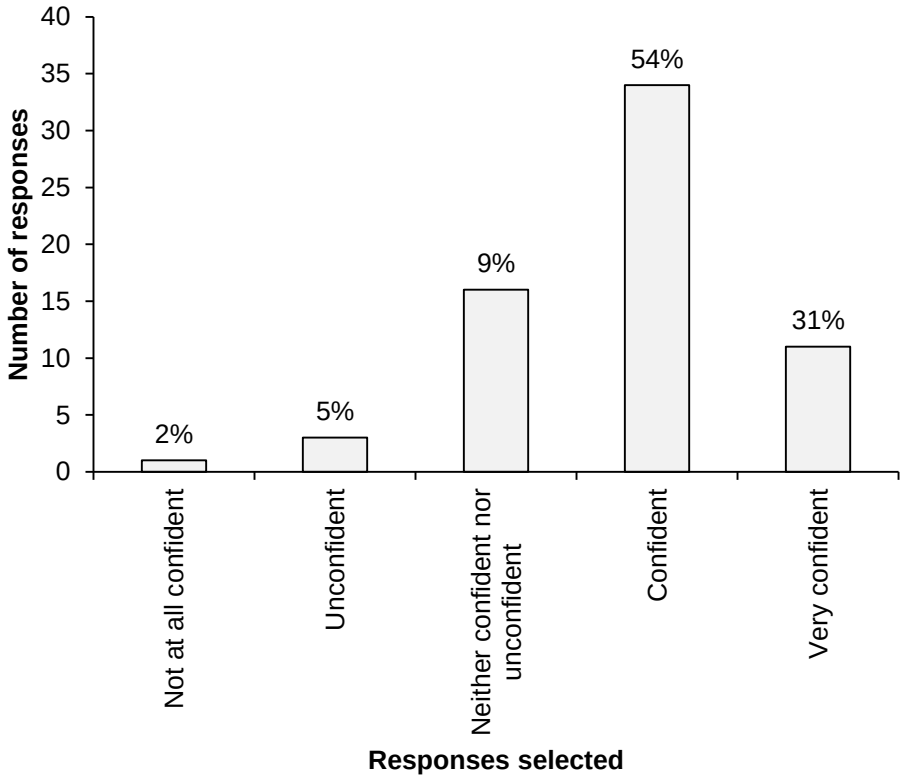

Figure 28. Responses to the question: How confident or unconfident are you in knowing when you are required to get a client's consent prior to you sharing their personal information with others? *N* = 65

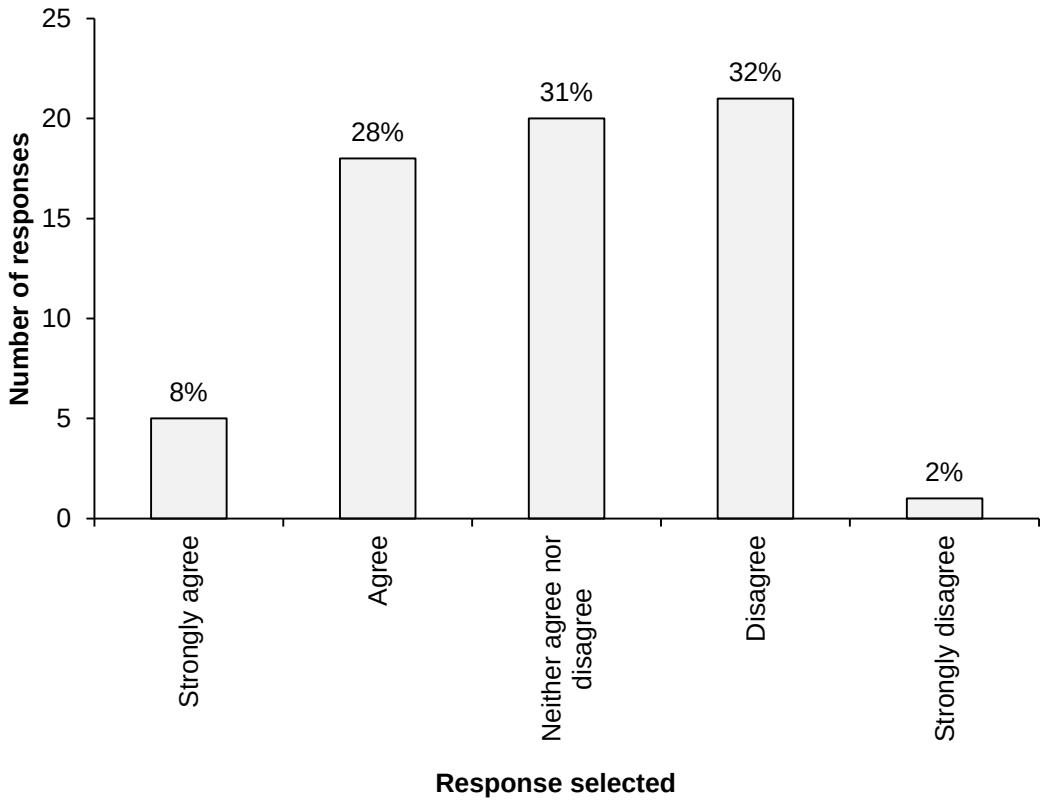

Figure 29. Responses selected for the question: Please indicate how much you agree or disagree with the following statement: "Information sharing between organisations should only be allowed with the informed consent of the client (i.e. even if the Privacy Act 1993 permits the information to be shared without consent)" *N* = 65

Seventy-four percent of respondents answered that their organisation has a formal system for managing information requests while 23% said they do not and 2% said they do not know. Forty-two percent of respondents said that their organisation requires requests to be recorded in a register or similar while 36% do not and 22% do not know if this is required. Forty-eight percent of respondents said that their organisation have a system in place to ensure that a response to an information request is given in the required timeframe.[32] This was unexpected given that section 39 and section 40 of the Act outlines the mandatory timeframe for transferring or deciding on requests respectively. Only 38% of respondents said that their organisation almost always meets the timeframe required for responding to requests and 26% responded that they do not know if the timeframe is met (Figure 30).

[32] If the information to which the request relates is held by or is more closely connected with the functions of another agency, the time limit for advising the requester of that situation and transferring the request is 10 working days (section 39). Where a request is made directly to, or transferred to an agency that is able to respond, the time limit for deciding whether a request should be granted and the individual provided notice of the decision is 20 working days (section 40(1)). The agency may extend the time limit (section 41) and the time limit shall be effected by advising the requester of the extension within 20 working days. Privacy Act, 1993.

This may be a reflection of some organisations not having a system in place to manage requests.

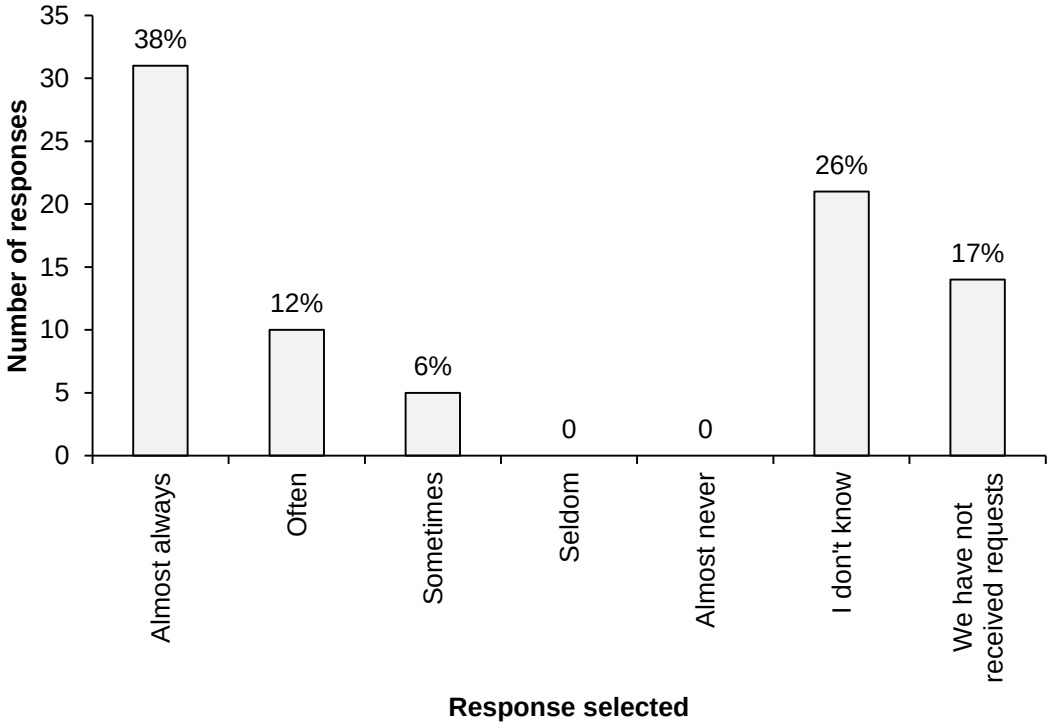

Figure 30. Responses to the question: How often does your organisation meet the time frame required? *N* = 81

When a request for personal information is made (by the client or another organisation), 37% of respondents answered that they are required to report the request, 34% said they are not required to and 29% said they do not know. Forty-two percent of practitioner respondents said they are required by their employer to consult with another staff member (i.e. supervisor, manager, privacy officer) about whether that information can be disclosed, while 31% said they are not required to and 28% do not know. This is indicative of non-compliance with the Act as pursuant to section 23, requests made to an agency are the responsibility of the privacy officer and it is their role to ensure compliance with the provisions of the Act. Furthermore, as aforementioned, given that nearly one third of respondents had not received training in the Act, this leaves the potential for information to be mistakenly disclosed or withheld. However, these results did not mirror those from the organisational level survey (Figure 31) where 85% of respondents said that their organisation requires staff members to consult with another staff member (i.e. supervisor, manager, privacy officer) about whether information can be disclosed if a request is made. This demonstrates a disconnect between organisational expectation and what practitioners actually do.

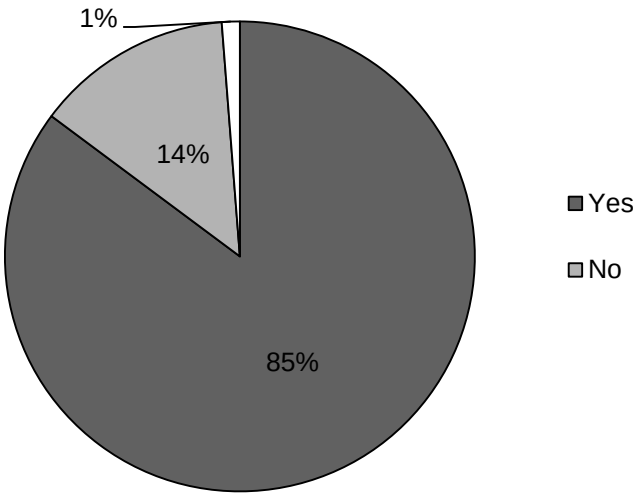

Figure 31. Responses selected for the question: If a request for a client's personal information is made (by the client themselves or another organisation), are staff members required to consult with any other staff member (i.e. supervisor, manager, Privacy Officer) about whether that information can be disclosed? *N* = 81

Practitioners were asked about potential barriers they may face when it comes to information sharing (Table 1). Most respondents (82%) agreed that they know when and what client information they are permitted to share. Twenty-nine respondents (45%) agreed that they have experienced a lack of response from other organisations when requesting personal information they hold about a client. Having insufficient time to ascertain if they are permitted to share a client's personal information does not seem to be a major barrier with only seven respondents (11%) agreeing at some level that this was a barrier for them. Seventeen respondents (26%) indicated some agreement with the statement that their professional code of practice prevents them from sharing information but similarly, 19 (29%) disagreed while 21 (32%) neither agreed nor disagreed that this was a barrier. Interestingly, the belief that a code of practice prevents them from sharing information is unfounded as per section 3 of the Act, information that is held by an employee of an agency in that person's capacity as an employee is considered to be held by the agency of which that person is an employee.

Table 1. Responses to the question: The list below identifies some potential barriers you might face around sharing client information with other organisations under the Privacy Act 1993 / another Act (law) or formal Memorandum of Understanding that is applicable to your organisation. Please indicate your level of agreement or disagreement with the following statements. *N* = 65

Answer Options	**Strongly agree**	**Agree**	**Neither agree nor disagree**	**Disagree**	**Strongly disagree**	**N/A**
I know when and what client information I am permitted to share	10	42	7	5	0	1
I've experienced a lack of response from other organisations when requesting personal information they hold about a client	12	17	14	17	2	3
There is insufficient time to ascertain if I am permitted to share a client's personal information	1	6	34	17	4	3
My professional code of practice prevents me from sharing information (e.g. The Code of Ethics of the Aotearoa New Zealand Association of Social Workers, Code of Ethics of the New Zealand Association of Psychotherapists etc.)	5	12	21	16	3	8

Approved Information Sharing Agreements

The number of respondents who were able to contribute to the data collected regarding ASIAs was low (*N* = 12). Nonetheless, the data that was collected is able to provide some insight. Only one third of respondents said they have read the AISA relevant to their organisation. The majority (58%) of respondents answered that they had not received any instruction/training from their employer on how to ensure compliance with their organisation's AISA. Only half of respondents answered that they have been issued with guidelines (i.e. written instructions or a pamphlet) for how to ensure compliance with their organisation's AISA. This is concerning given the requirement for training listed in the Information Sharing Agreement for Improving Public Services for Vulnerable Children whereby each party to the agreement must ensure that staff with access to personal information under this agreement either receive appropriate training and/or are issued with guidelines to ensure compliance with the agreement.[33,34] As seen in Figure 32, no respondents answered that they are very confident in identifying the circumstances in which they can share information under their organisation's AISA with 42% answering that they were confident and 58% not considering themselves confident (33% said they were neither confident nor unconfident and 25% said they were unconfident). One-third of respondents said that they have used their organisation's AISA to share client information while 42% said they have not and 25% responded that they do not know.

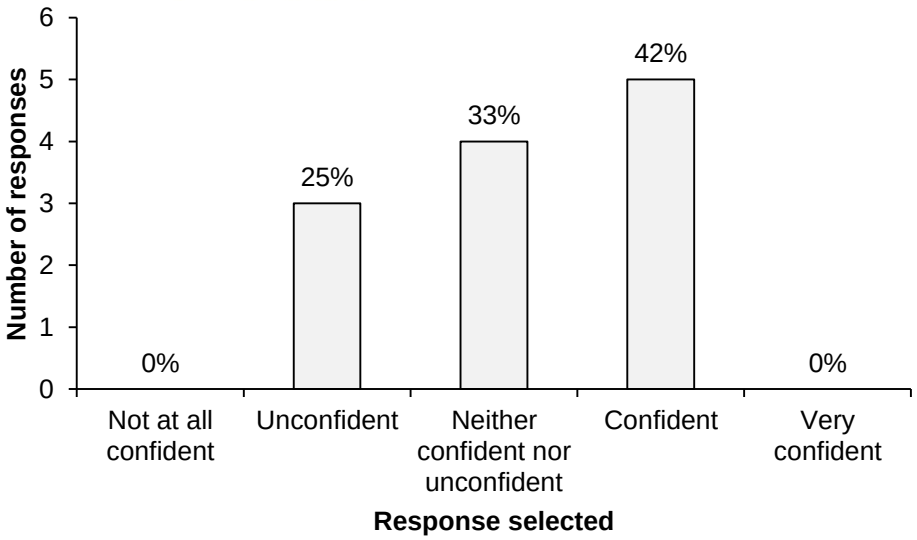

Figure 32. Responses selected for the question: How confident or unconfident are you in identifying the circumstances in which you can share information under your organisation's Approved Information Sharing Agreement? *N* = 12

[33] Information Sharing Agreement for Improving Public Services for Vulnerable Children, clause 9(5).
[34] Even if by chance the 42% of respondents who had received training in the AISA differed from those respondents who had received guidelines at 50%, this still leaves some practitioners who have received neither.

Three-quarters of respondents said they do not know what an ‘adverse action’ in terms of an AISA is. This is particularly concerning given that should an adverse action be identified, clause 12(3) of the Information Sharing Agreement for Improving Public Services for Vulnerable Children outlines the steps to be taken. If a practitioner does not know what an adverse action is, then it is unlikely they will be fulfilling the steps required by this clause and thereby be non-compliant with the terms of the agreement.

No respondent answered that sharing information with other agencies under an AISA is easy (Figure 33). Only 17% said that it is somewhat easy while 42% answered that it is neither easy nor difficult and the remaining 42% answered that it is somewhat difficult. This was unexpected as one of the very purposes of the Information Sharing Agreement for Improving Public Services for Vulnerable Children is to remove barriers to effective information sharing.[35]

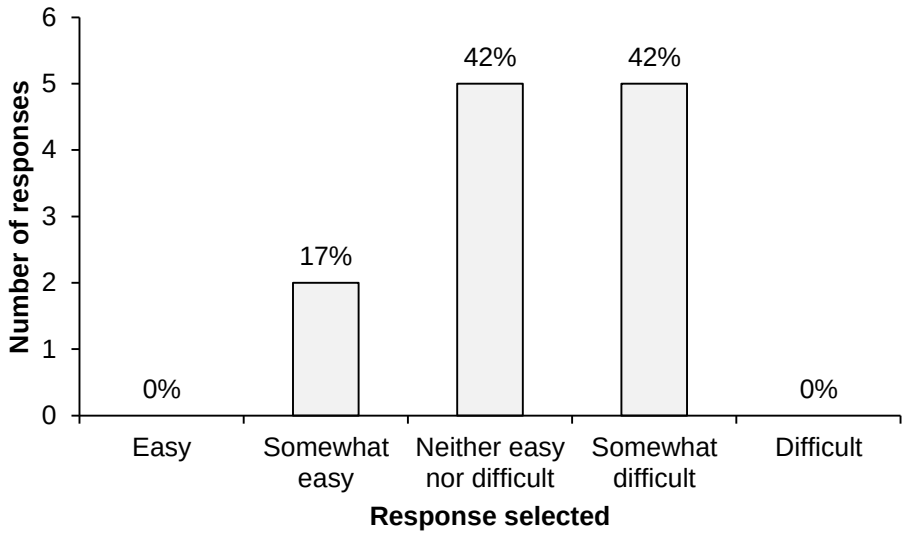

Figure 33. Responses selected for the question: Please indicate your response to the following statement: “Sharing information with other agencies under an Approved Information Sharing Agreement is:” *N* = 12

[35] Information Sharing Agreement for Improving Public Services for Vulnerable Children, clause 4(1)(b)

RESULTS AND FINDINGS PART TWO

It was clear from the participant interviews that practitioners and managers view the right to privacy as important and that the Act impacts on and "underwrites" the work they do. Participants at both levels expressed the sentiment that information sharing is an important part of working with a client but described this in the context of needing to maintain and protect client privacy. This was epitomised in a participant's statement "I just can't stress enough the importance of it. Of, people's privacy and confidentiality being you know upheld, but also where there's a need to share information that it's done in a way that keeps people's integrity". Another participant phrased it as needing to share and interpret information with "tika, pono and with aroha" (accuracy, sincerity and love/compassion).

As will be demonstrated in the following analysis,[36] most participants endeavour to uphold the principles of the Act and when that does not occur it generally stems from a lack of awareness or misconception. However, at times participants were more forthright, expressing a willing disregard for the information sharing exceptions. For example, one participant provided a case study:

> [I]f a client comes in… and he was supposed do a parenting programme as part of his compliance based on domestic violence. So, I said have you gone to your programme? And he goes yeah. And I said no you haven't because I've just spoken to the case worker and he said you haven't gone. Okay, so there's a sharing of information that allows me to know that. So what I do when I finish with the session is that I will email the other two or three providers and agencies. So clearly there's a sharing of information, so clearly there's tension with the Privacy Act in terms of sharing that...Understanding that if someone's coming in, and they're telling you this, you know already what is happening behind the scenes and where you will find a lot of issues or a lot of significant kind of failings is that where information is not shared. So, basically what we've done is that we will notify each other when that client has contacted our service and then update the collective service involved in that particular client. So that's those parts of the Privacy Act that resist information sharing, that is about improving health and safety and added value to whānau.

The participant described how the "collective" is not a management driven initiative (and is unknown to management of these organisations) but a frontline collaboration with other practitioners where sharing is "very much done discreetly". This disregard for the Act (and breach of Principle 2: *Source of personal information* and Principle 11: *Limits on disclosure of personal information*)[37] was not malicious but instead stemmed from a desire to act in what the participant deemed to be the best interests of his clients. The participant said how for most clients "going beyond the bounds of the Privacy Act could be great" and that where he feels that "sharing information is a life or death situation, *or it adds value to the care and support of whānau, well then yeah, I'll share it*" (emphasis added).

[36] The following themes are not presented in a weighted order. Additionally, there are instances where the gender of participants has been altered in order to protect confidentiality.
[37] Privacy Act 1993, s 6.

Training on the Privacy Act 1993 and privacy principles

"But it would be an easy trap to fall into, for people to make mistakes, because the training we get isn't very good".

Participants' responses regarding their training on the Act and privacy principles were mixed. Some said they had received training and described a comprehensive training strategy that included initial and refresher training as well as covering specific situations as they arose – "…different situations have come up, so it's like oh okay, we need to actually do a training on that". However, several participants expressed that they had not had any training or that they felt their training was inadequate. One participant who had received no training said that she thought training would be beneficial, not only for knowing what she could share but also so she was able to respond to agencies who would not share with her and hence be more informed in knowing whether they were correct or not.

One of the participants who said they had received no training was a frontline staff member from a government organisation who spoke elsewhere in his interview about how staff members "have to share a lot of information with other agencies". It is therefore alarming that he had not received any privacy training. As one participant who felt their training was inadequate said: "But it would be an easy trap to fall into, for people to make mistakes, because the training we get isn't very good". Another participant described how her training involved completing an online module "while you've got things going on, and you get through it and you have to get a certain percentage…they tick the box and say we've now trained you in that". She described how she did not consider this was the best way to learn and that "you're just doing it very quickly to get it out of the way and you're not getting input as such, you're just reading something on a screen. It's not a very good way of retaining information. It's not a very good delivery package I think. I see why the job does it because it's easy for them. But it's not very beneficial for us". Again, this participant was a frontline staff member at a government organisation and she too had spoken of frequently sharing information with other organisations. These comments may provide some explanatory value to the quantitative results where some participants reported they had received training in the principles but were not confident using them in practice or the occasions when their responses were inconsistent. For example, many survey respondents indicated that they were confident in knowing when they could release a client's personal information but many did not consider themselves confident when it came to identifying the circumstances in which they could withhold information.

One manager spoke about how her organisation was looking to implement an online course on the Act but she expressed a preference for face-to-face training: "However, to be honest, I would rather have on the ground training. It would be great for all the staff to go along with one person because the thing with the online one, okay that's fine, but the thing about sitting with people, especially in a group, people can learn off each other in situations, you know, and that interaction I think, face to face, is much better than online. I'm pretty sure online is much cheaper but I think I would rather have like a day or two-day

training on the Privacy Act because you can learn so much from other people's issues they have and the interaction, and you can ask questions, which online is a bit more tricky and have discussions and bring forward kind of made up scenarios and possibilities, some role play".

Another manager said that she did train staff but "not to a degree that probably I need to…" She went on to describe that if a practitioner has a registration board, then she thought they "should be up to the play". Another manager conceded that it was difficult to train staff "because I mean we don't all have a legal background, and we don't always have the ability to understand that grey area". Two other managers (and a survey respondent) commented how they drew on the assistance of the University of Otago law school staff in developing policies and undertaking staff training. One described this as "incredibly helpful". This may be indicative that the Act is difficult for some organisations to interpret, ensure appropriate training is provided, and that specialist legal assistance may be required. It could also mean that organisations are unaware of the resources made available by the Office of the Privacy Commissioner, especially when read alongside the survey result where only 29% of respondents had answered that their privacy officer had undergone training administered by the Office of the Privacy Commissioner (Figure 11).

Support from managers

"It would be really hard without them. Because you're having to make the judgement yourself as to whether you think it's the right thing to do and again, even if you take it to your manager so that…that call doesn't lie solely with you. It's almost a shared experience and it's better that way".

Many frontline participants spoke of consultation with their manager/supervisor in terms of information sharing. Participants spoke of having a "chain of command" (or as one participant termed it – "a chain of support") and that it was "helpful to know that there's somebody that you can go and ask". One participant described how "it would be really hard without them. Because you're having to make the judgement yourself as to whether you think it's the right thing to do and again, even if you take it to your manager so that…that call doesn't lie solely with you. It's almost a shared experience and it's better that way". Another participant said how she liked being able to "fall back" on her manager/supervisor for support. The survey results were such that 42% of practitioner respondents advised they are required by their employer to consult with another staff member (i.e. supervisor, manager, privacy officer) as to whether requested information can be disclosed while 85% of manager respondents said that their organisation requires staff members to consult with another staff member in those instances. Given the participant responses and survey results, it would be prudent for organisations to ensure managers and privacy officers are well-trained. Interestingly, less than a third of survey respondents answered that their privacy officer had undergone training administered by the Office of the Privacy Commissioner (as seen in Figure 11).

Giving a client access to their personal information

"We gather that information and give it to them. Because if it's under the Privacy Act and it's their own information, they can have it I guess".

In general, participants were well informed when it came to knowing that clients can access their personal information with none suggesting that clients could not access this information:

- "We gather that information and give it to them. Because if it's under the Privacy Act and it's their own information, they can have it I guess".

This was fairly consistent with the quantitative results where the majority of respondents (78%) indicated that they were confident or very confident identifying the circumstances in which they can give a client their own personal information.

As stipulated in section 23 of the Act, privacy officers are responsible for dealing with requests made to the agency pursuant to the Act and therefore requests for client information should go through them. Most participants spoke of having a process in place for client information requests:

- "That's got to go through our privacy officer first of all. We can't just randomly print off a page and give it to the [client], of their own file, that goes through our privacy officer first. They are always given. She plays the role like any other privacy officer to ensure that it's accurate and up to date and it hasn't got identifiable information about other people".

Additionally, most participants discussed how some information could be redacted prior to releasing client information citing reasons consistent with provisions of the Act such as information that would involve the unwarranted disclosure of the affairs of another individual,[38] or would endanger the safety of an individual.[39] However, one participant said she did not know what kind of information could be redacted and that it "would really depend on the client".

Two participants (from different organisations) spoke about soon to be implemented databases that would allow the client to access their information remotely "from the cloud system". One reason given for this was that one of these organisations does "collaborative note-taking" with clients and "it gives us a bit more transparency and it gives people the opportunity to look at their notes when they want to…" The other participant said how he would be able to "work across a collective really efficiently".[40] He also said how the database would allow individuals to "see their personal information, they can see what appointments they've got, because one of the biggest issues with individuals is that they don't have a history in their head of what they've had, where they've gone, you know, the

[38] Privacy Act 1993, s 29(1)(a).
[39] Privacy Act 1993, s 27(1)(d).
[40] The participant had previously described operating as a "collective" when working with the client whereby he informally collaborated with other agencies engaged with the individual in order to address their needs.

last ten years, what their NHI number is, actually what the name of the doctor was, you know. So, the whole point of this is to grow this software where they're able to do that. Well the doctor is able to provide a better diagnosis. Presently, arguably, you go to a doctor and all they know of your history is what you're telling them, or what they have of you. But if they're able to see a broad range of engagement, they can better assess you. Yeah, hence, *added value*" (emphasis added). While there would be advantages to these kinds of databases, if client information was provided in this way with constant access, organisations would require appropriate policies and safeguards, for example, to ensure third-party information could not be accessed. Furthermore, as aforementioned (page 21), agencies should be conducting audits of IT security of client information when it comes to keeping personal information safe and fulfilling the requirements outlined in Principle 5: *Storage and security of personal information*.[41]

One participant stated that when a client's information is prepared for them, their agency has "a form that outlines that the information is not to be used anything other than stated in the request. So it can't be used for legal reasons, or for any reasons that weren't stated for when it was asked for". The Act does not stipulate whether this kind of restriction can be made. Should a client express unwillingness to comply with the terms of the form and be refused access to their information, this is unlikely to comply with the Act as it is not one of the stipulated reasons for refusing access to personal information.

On not naming names

"I described the story and I said I think you might need to know dah, dah, dah, and we had something like a 45 minute chat, because they were very concerned with what they were hearing, wanted to ask lots of questions, and when I put down the phone neither of us had said the person's name. Neither of us had said the address, age, you know."

Misunderstanding of the Act became apparent when some participants spoke of withholding the client's name as being a method which permitted them to share information about that client. This was despite participants stating that they often provided sufficient details so the party they were speaking to would be able to identify the client and act on the information shared. The participants erroneously thought that by withholding the 'all-important' name of the client they were in compliance with the Act. This is despite the Act defining 'personal information' as being information about an identifiable individual[42] and therefore providing details as described is likely to be a breach of the Act.[43]

One participant (a manager) spoke of an instance when he shared information with another agency who a client was engaged with. Despite the client *explicitly denying* the consent to disclose the information, the participant did so justifying this because they did

[41] Privacy Act 1993, s 6.
[42] Privacy Act 1993, s 2.
[43] Privacy Act 1993, s 6.

not share the client's name: "I described the story and I said I think you might need to know dah, dah, dah, and we had something like a 45 minute chat, because they were very concerned with what they were hearing, wanted to ask lots of questions, and when I put down the phone neither of us had said the person's name. Neither of us had said the address, age, you know." The participant then described how the recipient of the information had gone on to discuss the issues raised in the phone conversation with the client and hence the recipient had obviously been able to identify who the client was. Another participant described how a practitioner may ring her for advice and she instructs the caller not to provide the family's name – "with a family you don't have the name of, you know, you can't identify the family, *hopefully*…" (emphasis added).

Another participant spoke about having been in meetings where she had "recognised the case studies" being used which made her "very uncomfortable because too much information is out there and I know instantly who they're talking about". She described how in these instances the client had not consented and yet identifiable information was being shared about them in these meetings, some of which were open to the public. This example demonstrates how simply removing the client's name is a fool's paradise in terms of maintaining privacy.

However, ignorance or disregard did not extend to all participants. One participant was clear to point out that "privacy doesn't mean just not mention any names. It is can that person be identified from that information or easily identified".

Consent

Consent was one of the most prominent themes to emerge from the interviews. Many participants described having consent from the client prior to sharing information. Pursuant to Principle 11: *Limits on disclosure of personal information*, if a client authorises information sharing, then this provides an exception allowing for disclosure.[44] Consent was often described as being a "big thing" that was important to establish.

In addition to gaining consent, telling the client when they were sharing information was highlighted as being important. Not only did participants see gaining consent and keeping clients informed as a way of ameliorating any issues with information sharing, they often described it as being part of forming a trusting and transparent relationship with the client.

- "And ensuring that we, if we do have to share information that we do that in a really transparent way…not let the Privacy Act, I suppose, my view is that, in the mental health and addiction sector, or counselling sector, we can get really caught up in trying to maintain privacy and confidentiality, but what we need to do is ensure that we are clear about what information we need to share. Yeah it's about being very considerate with people's privacy and respectful towards them with that".

[44] Privacy Act 1993, s 6.

So, at the core for some participants was that consent was part of whakawhanaungatanga (fostering the relationship with the client).

Some participants spoke of gaining the client's consent when the Act does not require it (i.e. in the case of a serious threat). Examples include one participant who said that "I think it's always best, even when we do have permission really, under the Act, to also get their consent as first case because I don't want them to feel like people are talking behind their back…" Another said that they would only give out information if the client wanted them to give it. These views mirror those expressed in the survey where some respondents expressed support for the idea that information sharing between organisations should only be allowed with the informed consent of the client (i.e. even if the Privacy Act 1993 permits the information to be shared without consent).

Most participants tended to view gaining consent as an event often taking place at the outset of their interaction with a client: "[Our clients] often they're involved with multiple agencies. So we really set that up from the start, that information is at times shared".

Some participants spoke about using a disclosure or consent form to get the client's consent. Again, this was usually said to be at the beginning of their interaction with the client: "I mean we've got a pretty clear guideline that we go through with the client when we get their consent, particularly when they first start with our agency".

Of concern was that one survey respondent commented "our consent to disclose form is ambiguous and confusing at best".

Some participants described how they thought gaining the client's general consent at the outset was a sort of catch-all for being able to share. However, some participants spoke about consent needing to be specific. For example, one participant said how "…we have to choose carefully what we require, really need, and what we ask them to consent to, and not generalise it either. It has to be specific". This belief was shared by others who expressed sentiments such as: "also being quite specific, so like I need to talk to somebody about this, I'm not going to mention any of that stuff…but we're going to talk about this bit" and "Because giving the whole client file is not relevant, so we need to know specifically what it is for". Another participant spoke about how their privacy waiver was "quite specific" and that they "try and be quite clear around consent". One participant spoke about how consent is obtained only for the specific reason for service and should other reasons eventuate then that is considered separate and another consent form is used. Two participants spoke about going back to the client and extending the consent that had already been given.

Thus while getting consent at the outset is certainly good practice, it is important to recognise that consent needs to be specific. Importantly, consent should also be an ongoing and iterative process whereby the client is kept informed and made aware that they are able to withdraw their consent to share even if this was initially one of the

conditions for service engagement.[45] For example, one participant spoke of being given consent and then the following day the client emailed to "take that consent back and I have to respect that because that's their choice…it's their right really, to take that back". Additionally, the client should also be made aware that they can change their mind and grant consent to share if they have previously refused. One participant described how a client may initially deny consent to share as when first asked, they may have been distressed "but actually when they are in a better space they actually really maybe do want the person to know. But if they are not asked again, if it's like a once ask/never ask again I think that defeats the purpose because people can change in terms of how that is etc.".

In general, participants spoke of few difficulties in obtaining a client's consent and that most "are really good at giving consent". This was often followed up with an explanation that the client is willing to give their consent if it is explained how information sharing is useful and that it will benefit them: "I try to set that up from the start, is that it is really useful for me and I think how you set it up can really help, just say look it's really useful to speak to this person and that person".

One participant spoke about working with young people and getting their consent to share information, particularly with parents. She explained "I find children and teenagers know that some information is actually useful for parents to know so they can help them". She gave an example of a recent session she had just had where she had obtained a client's consent and had asked "Can we share this with your mum, so she can help you?" and she said how "it was really useful to pass on that information, and the girl is absolutely fine with that. So I think *it is just about how you work that through with the* client" (emphasis added).

One participant however did say "If they don't want to consent, they don't want to consent. I mean there is nothing really we can do. You know, it's their choice. I mean, I guess then you can make it clear to them, I can't support you in this area, whatever area that is".

Despite having the client's consent, some participants spoke about how this was not a 'cure all' that allowed information to be shared as they were constrained by the other people working with the client and whether they were conversant with the provisions that permit information sharing. As one participant explained, "sometimes we get consent and it's not all fine because the other agency doesn't know how to interact within the Privacy Act as well. So for instance if we do have major problems I'll go, hello my name is [name] here, we've got a client in common who has given me a consent to talk to you guys. And I've had local, major agencies just about have a heart attack. You know they go 'I don't think I'm allowed to talk to you'". He explained how he gets "frustrated" as he has consent and he finds that some agencies are "extremely reluctant to engage because the problem of course they have is they don't know what they're allowed to tell me". Another participant shared a similar view saying: "The Privacy Act is pretty tight, and I think that practitioners actually use it as an excuse to be hopeless. Like seriously. Because you'll ring someone

[45] Acknowledging that this may mean that the client is no longer able to receive the service.

and ask questions about somebody else and whether you've got permission from that person or not, they just will knock it back on the Privacy Act basis".[46]

Some participants spoke about how, in some instances, rather than getting a client's consent to share information, they would refer the requester back to the client instead: "We generally would tell that, whoever is seeking information to talk to the person themselves".

Participants often cited not having a client's consent as a reason to withhold information. For example, one participant said how "making a referral to an organisation doesn't give you [an] ongoing right to know exactly what's happening unless the family approve of that or agree with that. So if they're not actively involved and there are no risks and the family have said, we don't need to keep them informed, then that's where it stands really". Other participants described situations where family members of clients had contacted them and how they made it clear to the family that they could not talk to them as they did not have the client's consent.

While these participants spoke of not sharing information with a client's family members when they did not have consent, others spoke of the difficulties this can bring. For example, how family members are often the "core supporter" for a person and when a client does not agree for them to share information with those family members, then that presents a challenge when it comes to keeping the client safe.[47] The participant went on to say that if there are safety concerns (their phrase) then they will share that with a family member. However, the Act provides an exception for sharing in regards to a "serious threat" rather than safety concerns. Another practitioner spoke at length about when practitioners refrain from sharing with family members in the case of a potential suicide when the client does not consent. In her opinion, practitioners refrain from sharing on the grounds that they "don't want to alienate the patient, we don't want to endanger the trust of that person because that person told us that in confidence and therefore we don't want to spoil that relationship so to speak". She spoke about how the family are often in the best position to provide a safety net for the person and sometimes the client may not be in the right frame of mind to give or refuse consent. She explained that she thinks that "if a person is over the age of eighteen I think clinicians are scared to share that information. They kind of use the Privacy Act to protect themselves rather than the patient" and that the practitioner is torn between two things: "One is fearing the wrath of the patient for sharing that information and in the other box is the wrath of the family for not sharing the information because the patient died". The participant posed the question: "Would you rather have a disgruntled patient or a dead one?" This kind of sentiment was shared by a

[46] See references to this issue in Lips, M., O'Neill, R., & Eppel, E. (2009). Improving information sharing for effective social outcomes. I.e. "the Privacy Act gets pulled out as a reason for not doing something" (p. 41) and "Furthermore, several respondents reported that many health practitioners were unwilling or unable to co-operate with other professional organisations (government or nongovernment), citing the Privacy Act as a blanket barrier to information sharing even when there was no sharing of personal details about a client involved (e.g. did they attend an appointment)" (p.64).

[47] This was referred to in terms of a barrier in a case study included in Lips, M., O'Neill, R., & Eppel, E. (2009). Improving information sharing for effective social outcomes. "For example, parents are expected to care for people with mental health conditions, but are not entitled to health information about them once they are legally adults" (p. 41).

participant in a case study examined by Lips, O'Neill and Eppel (2009): "The bottom line is that I would rather be hauled in front of the Privacy Commissioner, than in front of the Coroner's Office" (p. 35).[48]

Another participant said that "I just think that sometimes there needs to be more flexibility when families are concerned" while another participant took a different perspective describing how "family members say 'why you didn't tell me, why wouldn't you tell me what's happening with this person, why can't I know'" and this presents an opportunity for the practitioner to go to the client and explain how a family member is really concerned/stressed about them and how this really links to transparency with the client. He said "There is too much [sic] people talking behind closed doors with peers and some family members…and that's not going to work not just because of the Privacy Act issues, something that happens too much, but the problem is that transparency to trust them can really be broken down" and this can impact the trust between the client and practitioner and limit progress. As he phrased it, "Cohesion goes so far but the fact is in order for someone to move forward in some shape or form they have to feel they can work with someone to do that".

The view that there should be more flexibility when it comes to sharing with families was not universal with a participant talking about how "that's information that they can ask them directly, and the [client] can choose whether or not he shares that information…None of us share everything with our families…even if it's relevant in terms of, especially under a lot of mental health cases, they still have a right to privacy. Just because somebody is not quite right, does not take away their rights. So they still have a right to that. And we can't share that information, they need to do that themselves, or allow us to do it".

Informal information sharing

"And networks, informal information, well I mean you get it all the time".

While consent featured prominently and how acquiring consent was generally easy, it was surprising that another theme to emerge was informal information sharing – "And networks, informal information, well I mean you get it all the time". There was consensus amongst participants that informal information sharing is common and seems to take place by way of "informal chats" or "little conversations" between other professionals and with the public. Although participants were quick to acknowledge that informal sharing takes place, their responses to this were mixed. Some did not acknowledge that this type of sharing was counter to the principles of the Act while others acknowledged that it was "probably skating around or skirting around, whatever the expression is, certain legislation". Some participants denounced this kind of sharing and their explanations were indicative of compliance with the Act – "basically you just take it with a grain of salt and walk away and don't feed into that conversation"; "staff are quite good at knowing that the information they've received is outside of the Privacy Act, or a breach of the Privacy Act,

[48] Lips, M., O'Neill, R., & Eppel, E. (2009). Improving information sharing for effective social outcomes.

and they would normally say something about it. And they would make absolutely sure they don't act on that information, you know you can't un-know [sic] it. But they wouldn't act on it or share it further". Another participant gave an example of what staff do when someone asks about a client they are working with: "We say, well just need to tell you that, for example, if you would share things about Bob we would be passing that on to Bob but we can't share things with you unless Bob is happy for us to do that. We're happy to contact Bob and say 'look Tom has contacted us and would like to talk about bla bla bla, what would you like to do with that?' So it's really important for us. There's not a secret squirrel type of stuff that's behind".

For other participants however, there was a clear tension in that while they acknowledged informal sharing is not appropriate they felt that on the other hand, the information acquired this way can be very useful. This is exemplified in the following example:

- "I would be lying if I said look there weren't conversations, phone conversations, that highlighted some things and whatever but, you know, you can't, it might give you a better understanding of what you're doing…and they may add to what you can do to help without directly having anything on paper or using that information irresponsibly".

While receiving unsolicited information is not in itself a breach of the Act, what some participants were demonstrating was that evidently others are breaching the Act, in some cases wilfully, in order to share this information – "we do obtain information in manners sometimes that I think put that person in breach of the Privacy Act, the person we're getting the information from"; "You can go to a certain [organisation] and they will tell you something. And they might go, do a wink and say, I shouldn't tell you but as it's you, such and such…" Furthermore, once acquired, other obligations under the Act are engaged. For example, Principle 8: *Accuracy, etc, of personal information to be checked before use* requires that the agency not use that information without taking reasonable steps to ensure that the information is accurate, up to date, complete, relevant, and not misleading.[49] More than one participant described the client being asked to ascertain if there was truth to the information received. This however was the exception, as other participants did not alert the client to having received information or check if it was accurate with one saying it "doesn't mean that I'm going to go to that client and say whatever that professional said, but it does mean I've got a little bit more in my knowledge of them" and another saying that she did not do anything with the information except in changing how she treated the client.

Given that participants did not generally find getting the client's consent to share information to be difficult and consent was stressed as being part of forming a trusting and transparent relationship, it was surprising that informal sharing appeared to be so prevalent. Using informal information was not limited to those participants in the present study. The distinction between formal and informal information also emerged amongst frontline government staff in the case studies examined by Lips et al. (2009). Informal information was described as "that which is unwritten and exchanged usually directly

[49] Having regard to the purpose for which the information is proposed to be used. Privacy Act 1993, s 6.

between professionals (either individually or in groups) but is neither recorded nor in many cases acknowledged as valid or verifiable evidence but nevertheless constitutes part of the knowledge base a professional has. Informal information is acted upon as 'real' information" and that it is a combination of informal and formal information "which forms the basis for professional judgments about operational practices on a daily basis" (p.61).[50]

Practical aspects of maintaining privacy

"Just because you know that when people are a bit more emotionally raw, or a bit more vulnerable they do tend to say a bit more, and quite often it doesn't need to be in public".

Many participants spoke about practical aspects in terms of maintaining privacy. These included comments about:

- Being wary of thin walls and noise travelling.
- Turning files backwards so client names are not visible.
- Ensuring papers or records are kept out of sight – "clear desk policy".
- Checking requester authenticity by responding to work email addresses or phone numbers when asked to share information.
- Password protection on electronic devices.
- Restricted access to certain information and varying levels of access on a 'need to know' basis (this also emerged in a cross case study analysis by Lips et al. (2009) – "There are strong boundaries around particular data sets, with strict protection by authorised personnel").[51]
- Not speaking to clients about personal information in front of others.
- Using a document destruction bin.

One participant explained their organisation used a receptionist who was situated within earshot of clients and so to ensure client information is not shared accidently, the client is given a piece of paper to write down their details and this is passed to the receptionist so they do not have to share their information aloud "Just because you know that when people are a bit more emotionally raw, or a bit more vulnerable they do tend to say a bit more, and quite often it doesn't need to be in public".

Some participants spoke about practical aspects of privacy being particularly important when it came to accessing mental health services. This was grounded in the stigma surrounding mental health and that others may see someone accessing mental health services.

Overall, participants were knowledgeable when it came to the practical and visible aspects of privacy and they took steps that were consistent with the obligations outlined in the Act

[50] Lips, M., O'Neill, R., & Eppel, E. (2009). Improving information sharing for effective social outcomes.
[51] Ibid.

in regards to storage and security of personal information.[52] This was compatible with the survey results where 98% of respondents said that their organisation has a policy about how client information is stored and 86% answered that their organisation has a policy about what happens to a client's personal information when it is no longer required.

Māori worldview

"I think something needs to be done with the Privacy Act in terms of Māori philosophical beliefs because I don't think that there's any flexibility in there… which makes things practically difficult."

One meaningful theme to emerge from discussion with Māori providers was the suggestion that the Act is at times incongruous with a Māori worldview. One practitioner conceded that in certain situations, the Act was breached in order to give effect to the Māori worldview "Even though it is personal private arguably, because it's whakapapa, it's *collectively owned*, I guess, is the way that we view it" (emphasis added). "I do think, and I think that probably we as Māori are a bit looser about overlooking the black and white nature of the Privacy Act". This participant described sharing information that was not detrimental to the people who own it and how the information sharing is in people's best interests and can be used to benefit whānau. Another Māori service provider echoed this view, describing how they think the difference for Māori is not whether the information is private, but whether or not sharing that information is detrimental to the person concerned. He also described how the ability to share information is "governed by the rules and regulations of the culture that we're in" and that the Māori perspective of health – Whare Tapa Whā – had been a catalyst to realising that information sharing is important. This person also iterated that "the ability to share information of a client to the whānau is important for the health and wellbeing of the whānau".

A third Māori service provider also spoke about the tuakana/teina relationship and information sharing. She provided an example whereby the grandparents of a child have been unable to get information from an organisation about a situation involving their mokopuna (grandchild) and have subsequently contacted the participant who provided some information to them. She then told the grandparents to contact the child's parent. So while this would be a breach of the Act,[53] it was considered by the participant to be a culturally appropriate response.

Notably one participant from a non-Māori provider expressed the concern that some clients do not want the *whānau* or *iwi* finding out what is going on for them and as such prefer to use non-Māori service providers.

[52] Privacy Act 1993, s 6.
[53] Assuming the individual concerned had not consented to the sharing of this information.

Perceived challenges to information sharing

Participants were keen to relay challenges that they perceive in terms of the Act and information sharing. These challenges were normally centred on:

- The inability to share information when they thought it would benefit the client.
- Information being withheld when sharing would benefit the client.
- Not knowing who to share information with.

The inability to share information when it would benefit the client

"Yeah I guess if you're wanting to provide a wraparound service, and each kind of agency, yeah, has that little piece of the puzzle, if you kind of shared that, you'd be able to give the person the best service".

The inability to share information due to restrictions within the Act was frequently cited as inhibiting positive outcomes for the client as summarised in the following quote "I think that the biggest challenge for us is the inability to share information about people who would probably benefit from that sharing".

One participant gave an example where a client's likelihood of committing a crime is escalating or they are "becoming destabilised, or they're back on the, the drink, or they're back on the drugs and we know that when they're intoxicated that they're more likely to commit crime" and then described how getting consent to share in this situation was problematic: "We can't always, when they're in that state, ask them for permission, because the permission they give, they'd probably, could later argue that they were intoxicated and gave the permission under duress or didn't understand or whatever. So it might be in their best interests, but they don't necessarily agree with that at the time". The participant explained that if they were able to share information with other agencies then a multi-agency approach could ensue i.e. Work and Income could release funding for the person to go to another rehabilitation program or a community constable could visit the person and provide support. This case study demonstrates how "obtaining an individual's permission may not always be possible or practical" which was highlighted in the Ministry of Justice Background Paper on Improving information sharing, inter-agency co-ordination and case management to address the drivers of crime as being a difficulty preventing disclosure.[54]

Another participant also referred to having problems when they were unable to share with other agencies and that this was where they had most problems with the Act. This participant explained how their organisation often finds themselves in a space where they acquire information from a client that the client has not shared with their counsellor, case worker or their GP. Often the client has accessed their service multiple times and hence they have a history of the person and "end up sitting on a lot of information that we know

[54] Ministry of Justice. (2010). Addressing the Drivers of Crime. Background Paper: Improving information sharing, inter-agency co-ordination and case management to address the drivers of crime (pp. 1-16).

would be very beneficial for [those organisations] to actually know". This participant also gave an example whereby in a meeting, a professional from a different organisation might talk about a client in terms of them being under a "very good wraparound service with a great case manager and they have got them nicely contained now and they are working on a good case management plan" but unbeknown to this professional, the client is actually engaging with the participant's organisation on a daily basis "and the reason why that to me is a concern is because the client's engagement with us will be undermining the case work".

A different participant describes the tension in this situation: "On one hand it inhibits a little bit of what we do but on the other hand it's our responsibility to ensure that we maintain the privacy of that [client] at all times".

Another participant thought the Act already had enough flexibility when it came to sharing information but thinks the provisions need to be clearer – "I think unfortunately it's been interpreted in ways that haven't been helpful. Because I think the Act actually allows for that discretion. I just think it's how it's enacted at times…"

Information being withheld when sharing would benefit the client

"It can be quite frustrating and it's like we don't want to know because we want to be gossips, or we're not going to use this information, but if you're sitting in a meeting and you know stuff that is really relevant and you're not able to share that, and you're doing it in a way that thinks you're protecting somebody, then actually you can be creating so much more risk, you know. And kids die from that. And adults suicide from that. And people get hurt from that. It gets frustrating".

Linked closely to the inability to share information when it would benefit the client was when information was withheld by other organisations that if shared could benefit the client and others. One description given was; "it can be quite frustrating and it's like we don't want to know because we want to be gossips, or we're not going to use this information, but if you're sitting in a meeting and you know stuff that is really relevant and you're not able to share that, and you're doing it in a way that thinks you're protecting somebody, then actually you can be creating so much more risk, you know. And kids die from that. And adults suicide from that. And people get hurt from that. It gets frustrating". Another participant said how she thought that people were "too scared to say anything because of the Privacy Act...Or they're going to have the skies fall on them, because they have shared information. And then somebody gets hurt. So I think the fear that they're going to, and know there's that whole conflict of do I share this information because if I don't I might get charged because something might happen you know…"

Another shared her frustrations when it comes to participating in meetings with other professionals when information has not been shared: "It's really hard when you're working with other agencies and they withhold hold information, well not in a way to kind of screw

you over as such. But they're just being really really careful and they're like 'no I can't tell you that' and that's quite frustrating because often that's the information that does need to be shared… So, that's definitely a challenge when agencies don't share the information, that's how families fall through the gaps and how action isn't taken quick enough".

Another participant described how her safety (and that of the client) was put in jeopardy because critical information was not shared. She went to see a client and when she arrived the client was in the midst of attempting suicide using a weapon. The participant was able to diffuse the situation but later found out that it was known that the client had a weapon and this had not been shared with the participant and she believed it put both her and the client at unnecessary risk.

Many reasons were given as to why information may not be shared with several people thinking that practitioners are "too scared to say anything because of the Privacy Act". One participant described how she had recently come from a meeting where members of an organisation refused to share information but as the participant phrased it, "They should be able to because legally they can but that [organisation] is so scared of doing the wrong thing and ending up in court that they make life difficult. It's not so much that they make life difficult but it's making it difficult for the client. Because we are all on the same page we would be able to do a better job for the client". One participant reflected that "there's always that innate feeling that you're not doing the right thing". These kinds of views lend support to Justice Minister Amy Adams' comment that "[t]here is a high level of misunderstanding and almost catatonia about sharing information".[55]

Another participant thought that "sometimes people hide behind the Privacy Act and really, it's not in the best interests and I think if you keep the client at the centre and say what is in the best interest for them, then you know, then that kind of guides the path". Other participants thought that it was due to misinterpretations or ignorance of the Act. For example, one said how he thought they "should know certain things…I mean communication between a lot of the agencies could be a lot better, and I don't know if some of it is because people are unsure of what they can and can't divulge or not, like me". Others shared this view saying "there's various interpretations I guess within agencies and I think that is one of these issues… or maybe misinterpretations of it" and "smaller providers…generally don't understand the Privacy Act...they know it at, I would say, probably at a lesser level". This idea of multiple interpretations of the Act as being a barrier to information sharing was identified by Lips et al. (2009)[56] and cited in the Ministry of Justice Background Paper on Improving information sharing, inter-agency co-ordination and case management to address the drivers of crime.

[55] Trevett, C. (2015, August 5). Adams tackles privacy paralysis: Information-sharing push for cases of domestic violence. *New Zealand Herald.* Retrieved from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11491957

[56] See Lips, M., O'Neill, R., & Eppel, E. (2009). Improving information sharing for effective social outcomes (pp. 1-93); Ministry of Justice. (2010). Addressing the Drivers of Crime. Background Paper: Improving information sharing, inter-agency co-ordination and case management to address the drivers of crime (pp. 1-16).

One participant attributed a lack of information sharing to the way that some practitioners "perceive organisations or how they see things from their own culture". She said how "too many kids die and they shouldn't have to, and they shouldn't need to. And people, and kids get hurt. And people know stuff's going on, and professionals know stuff's going on". A survey respondent said that "Differing cultural perspectives and practice" act as a barrier to information sharing.[57] Another participant gave an example where information was not shared but "if we had that good relationship we could have just shared information". These participants' views echoed one of the findings from the Ministry of Justice Background Paper on Improving information sharing, inter-agency co-ordination and case management to address the drivers of crime,[58] specifically that "poor relationships between agencies and professionals can also impede legally permissible disclosure…"

Some participants spoke about how they thought there needed to be more discretion in the Act to enable information sharing and that the Act "can make life a lot more complicated than it needs to be, I think. I think it's probably gone too far one way... I think there'd be ways that you could streamline that [information sharing], and make it a lot easier without cutting corners, not necessarily being dodgy about it".

Participants frequently spoke about how a lack of information sharing impacted their ability to do their best for the client:

- "Yeah I guess if you're wanting to provide a wraparound service, and each kind of agency has that little piece of the puzzle, if you kind of shared that, you'd be able to give the person the best service".
- "In a way, the inability to talk about individuals hamstrings the multi-agency approach to helping particular people. But you simply can't disclose that information".

Not knowing who to share information with

"But who do you share with? It doesn't say. I think the law perhaps needs to say, be clearer about that area".

While participants recognised there were instances where information needs to be shared, some explained that they were not always sure who the information should be shared with, "When it comes to sharing the information, it is not very clear what that means, so sharing the information…if the police gets somebody that is suicidal, who do they share that information with? Family, a hospital? It's vague to say the least" and "But who do you share with? It doesn't say. I think the law perhaps needs to say, be clearer about that

[57] The Ministry of Justice Background Paper on Improving information sharing, inter-agency co-ordination and case management to address the drivers of crime (2010) mentions how "Professionals may represent quite distinct cultures with longstanding views about what can or cannot be shared with other professionals." For a brief discussion on a non-sharing culture being a barrier to information sharing (within the Australian context) see Commonwealth of Australia, Australian Government Information Management Office. (2008). National Government Information Sharing Strategy: Unlocking Government Information Assets to Benefit the Broader Community. Retrieved May 1, 2016, from http://www.finance.gov.au/sites/default/files/ngiss.pdf

[58] Ministry of Justice. (2010). Addressing the Drivers of Crime. Background Paper: Improving information sharing, inter-agency co-ordination and case management to address the drivers of crime (pp. 1-16).

area". Another participant spoke of how in difficult situations, practitioners can be reluctant to ask whether they can share information – "People get too scared to ask. Because then they have to do something and they don't know what to do, or they don't know how to do it".

In an organisational sense, one participant spoke of their organisation being passed information by other organisations and individuals that their organisation "might not have a direct connection with" and they then have to tell them that it is "…not good enough to tell us about it, that they need to take the appropriate action."

Threshold for sharing on the grounds of preventing or lessening a serious threat

"So I know that if someone comes to me and threatens to murder their wife, and I believe that threat to be true, that I have every right to disclose that because there's a safety issue there".

Pursuant to Principle 11: *Limits on disclosure of personal information*,[59] disclosure of information is permitted if it is necessary to prevent or lessen a serious threat[60] to public health or public safety or the life or health of the individual concerned or another individual. Principle 10: *Limits on use of personal information* also holds that personal information may be used for another purpose than for which is was collected provided that the use of the information for that other purpose is necessary to prevent or lessen a serious threat.[61] Participants were generally well-informed when it came to acknowledging that they were able to disclose information on these grounds:

- "So I know that if someone comes to me and threatens to murder their wife, and I believe that threat to be true, that I have every right to disclose that because there's a safety issue there".
- "I also talk about risk issues if there's any significant risk issues…if you know, harm to yourself, or if someone else is hurting you then that really trumps privacy because we can't keep secrets that are unsafe".

While some participants spoke about how the threat needs to be "serious", many participants spoke about how a threat needed to be "imminent": "If somebody is at imminent risk, is the new wording if I remember correctly, you've got to share that information".[62]

---

[59] Privacy Act 1993, s 6.

[60] A serious threat means a threat that an agency reasonably believes to be a serious threat having regard to all of the following:(a) the likelihood of the threat being realised; and (b) the severity of the consequences if the threat is realised; and
(c) the time at which the threat may be realised per s 2(1) Privacy Act 1993.

[61] Privacy Act 1993, s 6.

[62] Note how the participant said that under the Act they have "*got to"* disclose in this instance. However, the Act does not require disclosure but instead permits disclosure. Another participant spoke of letting their client "know that under the Privacy Act I *need to* disclose information if their or other people's health is at risk" (emphasis added) – again the Act does not require disclosure and a third participant said how "*we have to* disclose". This is a mischaracterisation of the provision.

Some participants expressed that the requirement of a threat being 'imminent' posed a challenge and that this was a "grey area". One example given was: "And define imminent you know, somebody's left the office. They're not going to kill somebody as soon as they go out the door, but they've threatened to do something when they get home, which might be at 3 o'clock this afternoon, or you know. So, yeah define imminent".

The threat as needing to be "imminent" is however an outdated interpretation of the Act. The threshold was amended by the Privacy (Information Sharing) Bill 2011 and 'imminent' was removed.[63] The Act previously outlined that a threat to a person's life or health or to public health or public safety as having to be "serious and *imminent*" (emphasis added). Removing the need for imminence has expanded the potential for sharing and grants agencies discretion to share information where a threat is serious but not necessarily urgent. Hence participants who are under the misconception that a threat needs to be imminent are potentially refraining from sharing information when sharing is actually permitted and may be beneficial. This presents a major concern. One participant spoke about wanting the ability to share information when a client was at-risk of committing a crime (page 50) and said how she could "share information if there's imminent crime going to happen. But sometimes you need something a little bit more loose than that". Unbeknown to the participant was that the test was more "loose" than she described it.

Participants also described dealing with other organisations in regards to a potential serious threat to be problematic in some instances, for example "The difficulty once again is if it's interagency". The participant proceeded to describe how they would disclose to other agencies that a mutual client has been expressing very high levels of suicide ideation and has formed a plan and began to self-harm more severely. In this kind of scenario, the agency does not have the consent of the client to share this information (but they are permitted to share it under Principle 11)[64] and consequently, some agencies do not engage well "which is a little concerning to us because our bottom-line is the safety of the adult…you're not overriding the Privacy Act, the Privacy Act lets us do stuff like that but…I think they get too scared of it". Another participant described how she had a disagreement with another agency of a mutual client when she thought the threshold had been reached but they did not.

[63] The wording of the Health Information Privacy Code1994 was also updated to mirror the change.
[64] Privacy Act 1993, s 6.

Approved Information Sharing Agreements

"Everyone is on the same page, they all know what's happening, one plan for the one child".

While limited, the response to AISAs was generally positive with both participants who operate under one espousing the virtues of these new mechanisms for information sharing.[65] The participant who provided an organisational level perspective explained how he thought the AISA had "certainly helped in the message of some of the practitioners' fears around previously not sharing information and the repercussions of sharing information, and sharing information potentially inappropriately, or potentially where people have complained about it. It provides them with some protection in that regards". They also described how the AISA was "part of the general culture shift or towards the importance of sharing information when there is safety or vulnerability of a child which in the past has been quite difficult to unlock in certain parts of the children's workforce"[66] and that "It's not just about the AISA coming into being, it's actually about understanding that the appropriate times when information can and should be shared".

The frontline level participant said how she "can see the definite benefits to having this new process" and described how "getting all the information that you need about a family so you can put in the best plans, having that information definitely helps". She described how she is "finding the benefit of that already" and in the case of clients she is working with how the information shared "will be really helpful for getting a picture of what's been happening for this family and how we need to progress to help them". She spoke about how without the AISA, "you get little snippets of information and you're not aware of what another agency might be doing with the same family. You might not even be aware that another agency is involved unless the family has told you and they might be working to a plan" whereas when she is operating under the AISA, "everyone is on the same page, they all know what's happening, one plan for the one child". While both participants pointed out the benefits of sharing under the AISA, they caveated this by explaining that due to the recency of its implementation, "its effectiveness is kind of yet to be determined" and that while systems were still being put in place, "it's really hard to progress". Additionally, the frontline level participant described how as some people are "new to this process…some people can be quite, a little bit cagey you know…so they don't want to share their information…there is still a lot of people out there that don't understand and may be a little bit negative with this new process".

---

[65] Two participants were able to comment on AISAs: one participant was a practitioner and the other participant was a manager (therefore providing insight at a frontline and organisational level respectively).

[66] The Ministry of Justice Background Paper on Improving information sharing, inter-agency co-ordination and case management to address the drivers of crime (2010) mentions how "Professionals may represent quite distinct cultures with longstanding views about what can or cannot be shared with other professionals." For a brief discussion on a non-sharing culture being a barrier to information sharing (within the Australian context) see Commonwealth of Australia, Australian Government Information Management Office. (2008). *National Government Information Sharing Strategy: Unlocking Government Information Assets to Benefit the Broader Community*. Retrieved May 1, 2016, from http://www.finance.gov.au/sites/default/files/ngiss.pdf

In terms of operational difficulties, the organisational level participant spoke about challenges regarding "the number of case management systems that actually exist…there are multiple systems within that system" and the difficulties that this creates. This participant provided an example of working with an organisation that has "more than eight different health systems or case management systems that hold different pieces of information about one person". When asking that organisation for information, it then has to come from "a variety of systems and then the sense making of that information is a challenge". They went on to give multiple situations including "what might be simple for a clinician to read and understand from a health perspective, might be quite different [for someone] in another profession that doesn't necessarily understand the terminology or the language that's specific to a particular health profession. So, just being lumped with a whole lot of file information, you run the risk of just simply not understanding it. And the volume of it, there could be a huge amount of information – how do you know what's relevant and what's not?...Who translates what actually what it means? It's one thing to have a bunch of information; it's another thing to understand what it means". The participant explained how he thought this issue is one that "really stands in the way of great information sharing" and a "risk when it comes to information sharing actually being useful". He also said that "you need the resource in behind the information sharing so there actually has to be people committed to providing that information in a comprehensive way and in a way that's understandable. And, if there's not going to be investment in that or commitment to doing that, then information sharing is going to be forever clumsy and not utilised in the way that it needs to be". The participant thought these concerns could be mitigated by "having a clinician doing a review of all the information across the systems and putting a synopsis or a summary together of the key things, you know, from a clinician's point of view where they actually understand the information that they're reading, and they understand the audience that they're sending it to, then it's far more valuable".

This participant reiterated resourcing being a challenge elsewhere in his interview, saying that challenges "sit around resourcing it and who's going to pay somebody to do that" and that they were keen to recognise that "information sharing is really important and central to how we need to be working in the future but alongside that there's a real lack of thinking about actually how it will work. And how it can be logistically and practically feasible…because we don't have the resource ourselves, to be able to work that out, and we don't have the control over the agencies to dictate to them as to what they do".

In response to being asked whether she had to be specific when requesting information, the frontline level participant explained she received "a lot of health information and hospital information" and that the whole file is made available to her to access. This seems counter to the provision in the Information Sharing Agreement for Improving Public Services for Vulnerable Children which outlines that "All practicable steps will be taken to ensure that any personal information shared is accurate *and the minimum information necessary to achieve the purpose of the request*" (emphasis added) and the principle that information sharing under the agreement shall be *relevant, necessary and proportionate* to

the circumstances and needs of vulnerable children and their families (emphasis added).[67] Additionally, the organisational level participant spoke about how it is hard for practitioners to "know what is relevant and what's not. There haven't been guidelines as far as I'm aware set up around you know, say we want to get all of the appropriate information around a child and their family members within the household from health, well what exactly do we mean by that? Do we want the dental records for every single person in the house, yes or no, and there's a whole lot of things that we may or may not want, but we're not clear ourselves in terms of what we think we need and what we know we don't need. And that's the challenge of working in a multidisciplinary context". Reading the AISA, it does specify what personal information may be shared (to a degree), for example in terms of health, the parties may share "information about a child's physical or mental health, which may indicate that the child has been abused or neglected or is at risk of abuse or neglect"[68] and "information about whether a parent or caregiver of a child has a mental illness".[69]

So while AISAs remove some barriers to information sharing (as outlined as an objective of the Information Sharing Agreement for Improving Public Services for Vulnerable Children),[70] the agreements can also replace old barriers with new ones.

Whether the training is appropriate and the obligation regarding training is being met is unknown. The frontline level participant said that she had received no training and when asked if she had read the AISA, replied that she had "scanned it". The Information Sharing Agreement for Improving Public Services for Vulnerable Children requires staff operating under the AISA to be appropriately trained and/or issued with guidelines to ensure compliance with the agreement.[71] The organisational level participant said "I'm not aware of a specific training module, around the AISA specifically, I am aware of a training module in relation to information sharing" and that "yes there is information provided, whether or not it's absolutely effective in achieving the kind of understanding that we'd want, I don't know, we haven't measured that. But the information is there".

Both participants saw value in expanding the current AISA they operate under to include non-government organisations with one commenting "So I think where there's been significant involvement of an NGO, then the ability to request that information under the terms of the AISA would be beneficial, definitely". While the other participant shared this view on the grounds that it would be more efficient time-wise, she cautioned that she thought there were some people who are not adequately informed on consents and information sharing so there was the potential for it to "become unsafe…"

[67] Information Sharing Agreement for Improving Public Services for Vulnerable Children 2015, clause 10(5) and clause 6(d).
[68] Information Sharing Agreement for Improving Public Services for Vulnerable Children 2015, clause 7(1)(e).
[69] Information Sharing Agreement for Improving Public Services for Vulnerable Children 2015, clause 7(1)(k).
[70] Information Sharing Agreement for Improving Public Services for Vulnerable Children 2015, clause 4(1)(b).
[71] Information Sharing Agreement for Improving Public Services for Vulnerable Children, clause 9(5).

Research limitations

It is acknowledged that multiple limitations potentially influence the robustness of this project and the conclusions drawn.

One is the way participants were recruited, specifically in the wording of the invitation to participate. The invitation outlined that the project was researching the way in which practitioners and senior practitioners/managers understand and apply the principles of the Act, particularly when it comes to sharing information. This could unintentionally exclude people who thought that they could not participate on the grounds that they did not know about the Act. This was exemplified by some participants who shared with the interviewer that they were unsure on the usefulness of their participation as they did not know about the Act. Consequently, the results of this study may not accurately capture the number and insights of practitioners/managers who were not versed in the Act (and thought they were not suitable to participate) and hence the results could potentially exaggerate the knowledge and competency of practitioners/managers as a whole.

Another limitation of the project is that one of the objectives was to measure competency. Ideally competency would have been measured against an objective standard. However, to do this would have required a test format rather than a survey instrument. This was not done as it was anticipated it would result in reluctance from participants as well as difficulties formulating questions that were relevant to all participants. Instead, self-reported data in the form of perceived or subjective competency was measured, primarily by asking participants to rate their confidence in applying certain privacy principles. This is inherently problematic as a participant may perceive themselves to be 'very confident' when in practice they are not compliant with the Act and thereby misstate their ability. To partially mitigate this, interviews provided a less structured setting where a participant's knowledge and competency could be more thoroughly and accurately gauged.

One limitation that arose during the interviews was that there were times when participants were reluctant to share examples or case studies as they were constrained on privacy grounds. The irony of this is duly noted.

Another limitation was the lack of data regarding information sharing in terms of AISAs as the number of respondents who were able to contribute to the data collected regarding ASIAs was low. This was likely due to a number of factors including:

- Only three AISAs are currently in effect.
- The Information Sharing Agreement for Improving Public Services for Vulnerable Children has initially been limited geographically to Hamilton, Canterbury and Counties Manukau.
- The introduction of AISAs is fairly recent (2014 and 2015).
- As of May 2016, only government agencies are parties to AISAs.

- Some AISAs are applicable to industries not canvassed by this study.[72]

It is suggested that further data is collected when AISAs have been in use for a longer duration and extended to other areas, in order to establish if the results of this study are still pertinent and generalisable.

[72] I.e. the Information sharing agreement between Inland Revenue and the Department of Internal Affairs 2014.

CONCLUSIONS AND RECOMMENDATIONS

From the array of themes that emerged from the interviews coupled with the survey results, a variety of conclusions and recommendations can be made. It is acknowledged that no recommendations will be a panacea but may go some way to improve competency and compliance with the Act.

The findings from this research show that both agencies and practitioners are conscious about the need to protect client information and while at times they act upon this need, there are also instances where they fall short. Furthermore, they are faced with various challenges in terms of privacy and information sharing.

It is evident that agencies and practitioners are generally competent when it comes to fulfilling some of their obligations outlined in Principle 5: *Storage and security of personal information*.[73] However, agencies should be made aware of the potential need to conduct audits of their IT security of client information in order to keep personal information safe (especially for those agencies using a cloud-based system). Agencies should be informed of the technology guidance section on the Office of the Privacy Commissioner website.

Both the quantitative and qualitative components of this research show that agencies are not adequately training staff. Knowledge gaps were apparent, particularly as many participants upheld the outdated belief that a 'serious threat' needed to be 'imminent' and that participants were not always confident when it came to applying the privacy principles and did not find them easy to apply in practice. Furthermore, training/instruction to staff members on when another Act or formal Memorandum of Understanding may apply that affects information sharing is not always being provided.

It is therefore recommended that organisations adopt a more rigorous training approach and that all staff members who encounter personal information are trained in the privacy principles and any other relevant legislation or formal agreements concerning information sharing. It is suggested this training include examining case studies and practical application of the privacy principles including when information can be withheld and how to share information while still complying with the Act. Related to this, it appears few organisations are taking advantage of the free training opportunities and resources, including a range of e-learning modules, available from the Office of the Privacy Commissioner. It should be noted that while e-learning has its benefits (such as being available any time, from anywhere) online training was highlighted by some participants as not being their preferred way to learn. It is suggested that online training is offered in conjunction with other formats such as on the ground training.

In order to meet the obligations of having a privacy officer, it is recommended that all agencies are advised on this requirement and that the benefits of having someone in the role are promoted. As indicated in the interviews, participants appreciated being able to

[73] Privacy Act 1993, s 6.

rely on someone else when it came to privacy issues so it is important that a) the agency has a privacy officer and b) the privacy officer is well-informed in the Act and made aware of the training opportunities offered by the Office of the Privacy Commissioner. Staff members should be made aware of who the privacy officer is and their role.

It is suggested that education occur at an operational level whereby agencies are instructed on their obligations under the Act, how they can meet those and incorporate them into organisational policies and culture. For example, a policy regarding information requests that incorporates a system to ensure information requests are dealt with in the set timeframe. Agencies should be informed of the 'How to comply' section on the Office of the Privacy Commissioner website along with further resources made available such as the Privacy Statement Generator. It is envisaged that competency at an organisational level will filter down and have effect at a frontline level, particularly as practitioners often seek support from their managers. It is also recommended that as part of their policies and training, that there are processes to combat informal information sharing and all staff are explicitly instructed about this and trained how to acquire the type of information shared in an informal setting through means that are compliant with the Act (such as getting consent). Additionally, agencies should examine their consent forms to ensure they are specific and advise staff that they can go back to the client to discuss consent when it is pertinent along with using consent as part of forming a trusting and transparent client-practitioner relationship. Education should also occur regarding what is meant by 'identifiable information' and that this is more than just naming the individual.

In terms of a Māori worldview and privacy, while further analysis of this is beyond the scope of this research, it is suggested the issues raised warrant further exploration, particularly in light of the principles of Te Tiriti o Waitangi / The Treaty of Waitangi, specifically *tino rangatiratanga* or self-determination.[74]

While the introduction of AISAs is recent, a small number of conclusions can be drawn. It is clear that AISAs are being used to facilitate information sharing as well as helping to alleviate fears around information sharing. This may be resulting in a culture shift that is more supportive of information sharing. However, AISAs are evidently not a panacea for issues surrounding information sharing and present their own array of challenges. These include difficulties when trying to acquire information from multiple systems, high volumes of information being obtained without the necessary skills to interpret the information and resourcing difficulties. One participant's recommendation worth exploring is assigning a suitably knowledgeable person to review the client information, interpret it and provide an assessment or profile of the information for the recipient. However, more familiarity with the terms of the agreement may also help alleviate issues in regards to the volume of information being received.[75] Related to this, it is recommended that all staff members working under the AISA are trained in its use as required by the terms of the agreements

[74] For discussion on tino rangatiratanga in the social work discipline see Hollis-English, A. N. (2012). Māori Social Workers: Experiences within Social Service Organisations (Master's thesis, University of Otago, 2012) (pp. 1-264). Dunedin: University of Otago.

[75] See Information Sharing Agreement for Improving Public Services for Vulnerable Children 2015, clause 10(5) and clause 6(d).

and that this training is comprehensive so staff can fully utilise the agreement while complying with the provisions. Furthermore, agencies and practitioners should utilise the AISA guide 'An A to Z of Approved Information Sharing Agreements (AISAs)' produced by the Office of the Privacy Commissioner. It is also recommended that funding is invested into resourcing a more useable system to share information and that the possibility of including non-government organisations as parties to the agreements is considered.

Some of the issues identified in this report may be ameliorated by the new proposals suggested following the Modernising CYF Expert Panel review.[76] The Minister for Social Development established the Expert Panel "with a mandate to determine how to tackle this most pressing issue that faces contemporary New Zealand: How can we transform the lives of our vulnerable children once and for all?" (p. 3). In the Expert Panel Final report, some of the recommendations related to privacy and information sharing. The report states that "An effective and robust case management system for the department is critical and will require the replacement of the existing case management system CYRAS, which lacks many of the necessary features" adding that: "CYRAS does not enable information sharing with external agencies and providers" (p. 122).

The Modernising CYF Expert Panel review report acknowledged that "[t]here is broad agreement that many of the professionals working with children, young people and families are unclear about what information they are allowed to share under this framework, with whom, and in what circumstances. There is also agreement that this has led to some practitioners defaulting to not sharing information because of that uncertainty, rather than pushing the limits of what they can share under the current settings, which has been to the detriment of vulnerable children and young people" (p. 154).

The report recommended that "a new high-trust information sharing system that is connected across agencies, partners, families and caregivers, brokered by a Child Information Management system, with a consent-based approach" is implemented (p. 122). This system is to be implemented along with a reformation of the Child, Young Persons and Their Families Act 1989 and as part of this, the formation of an information sharing framework within the Act "that would create a clear expectation that any individual discharging functions associated with the objectives of the Act should share or have access to personal information about a child or young person necessary to promote the safety and well-being of that child or young person" (p. 154) and "if information is to be shared without consent, this should only be where the practitioner believes that the benefits of information exchange to a child or young person outweighs any potential negative impacts, taking into account the level of sensitivity associated with the type of information being exchanged and that anyone acting in good faith under these provisions should be protected from any civil or criminal action, or any professional disciplinary action" (p. 155).

[76] Modernising Child, Youth and Family Expert Panel. (2016). *Expert Panel Final Report: Investing in New Zealand's Children and their Families* (pp. 1-300) (New Zealand, Ministry of Social Development). Wellington.

These types of recommendations may make people more willing to share information and reduce the "almost catatonia about sharing information" as identified by Justice Minister Amy Adams and in interviews with participants for this project.[77] It would also allow information sharing when it is in the client's best interest which was a sentiment that often emerged during the interviews. However, as the proposals only seek to make changes around vulnerable children, then this would mean that the potential benefits of the reforms would not be extended to the adult population. It is recommended that similar changes to the Privacy Act 1993 are considered in line with those proposed for the Child, Young Persons, and Their Families Act 1989.

The report also identified recent changes to information sharing provisions regarding vulnerable children and young persons as adopted in New South Wales and Scotland.[78] One of these changes included changing the threshold for information sharing in cases of 'serious threat' to promoting safety, welfare and well-being. This change may act as an impetus for a cultural change around information sharing and allow for sharing when obtaining consent is not practicable. This legislation is in relation to children but it is suggested that the same benefits could extend to the adult population.

Until macro level changes are implemented such as those proposed by the Modernising CYF Expert Panel review, it is recommended that short 'go-to' guides on information sharing and certain privacy principles are produced. The guides should be written in a manner that is easy to understand (i.e. avoid legalese), utilise case studies and possibly flowcharts. The guides should incorporate resources already available on the Office of the Privacy Commissioner website.

[77] Trevett, C. (2015, August 5). Adams tackles privacy paralysis: Information-sharing push for cases of domestic violence. *New Zealand Herald.* Retrieved from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11491957

[78] Children and Young Persons (Care and Protection) Act 1998 (NSW), ch 16A; Children and Young People (Scotland) Act 2014, s 26.

REFERENCES

Legislation and government documents

Cabinet Manual 2008.

Children and Young Persons (Care and Protection) Act 1998 (NSW).

Children and Young People (Scotland) Act 2014.

Child, Young Persons and Their Families Act 1989.

Health Information Privacy Code1994.

Information Sharing Agreement for Improving Public Services for Vulnerable Children 2015.

Information sharing agreement between Inland Revenue and the Department of Internal Affairs 2014.

Privacy Act 1993.

Other references

Commonwealth of Australia, Australian Government Information Management Office. (2008). National Government Information Sharing Strategy: *Unlocking Government Information Assets to Benefit the Broader Community.* Retrieved May 1, 2016, from http://www.finance.gov.au/sites/default/files/ngiss.pdf

Children's Action Plan. (2016, April 28). Sharing information - Approved Information Sharing Agreement. Retrieved April 30, 2016, from http://childrensactionplan.govt.nz/supporting-childrens-teams/info-sharing/

New Zealand, Children's Action Plan. (2015, November). *Frequently Asked Questions about Information Sharing in the Children's Action Plan*. Retrieved April 30, 2016, from http://childrensactionplan.govt.nz/assets/CAP-Uploads/AISA/FAQs-about-information-sharing-November-2015.pdf

El-Gamel, N. (2016, January 8). Problem gamblers' privacy breached when list tossed in footpath bin. *Stuff.co.nz*. Retrieved April 30, 2016, from http://www.stuff.co.nz/national/75689173/problem-gamblers-privacy-breached-when-list-tossed-in-footpath-bin

Hollis-English, A. N. (2012). Māori Social Workers: Experiences within Social Service Organisations (Master's thesis, University of Otago, 2012) (pp. 1-264). Dunedin: University of Otago.

Horizon Research Limited. (2015, December 7). Warning to companies: 78% want private data protected. Retrieved April 30, 2016, from https://www.horizonpoll.co.nz/page/422/warning-to-c

Levy, D. (2012, August 23). Cavalier attitude lead to NZ's biggest privacy breach. *The Dominion Post.* Retrieved April 29, 2016, from http://www.stuff.co.nz/dominion-post/news/politics/7530166/Cavalier-attitude-lead-to-NZs-biggest-privacy-breach

Lips, M., O'Neill, R., & Eppel, E. (2009). Improving information sharing for effective social outcomes.

McLeod, H. (2015, November 14). Invercargill woman slams CYF for privacy breach. *Stuff.co.nz*. Retrieved April 29, 2016, from http://www.stuff.co.nz/national/74029026/invercargill-woman-slams-cyf-for-privacy-breach.html

Ministry of Justice. (2010). Addressing the Drivers of Crime. Background Paper: Improving information-sharing, inter-agency co-ordination and case management to address the drivers of crime (pp. 1-16).

Modernising Child, Youth and Family Expert Panel. (2016). *Expert Panel Final Report: Investing in New Zealand's Children and their Families* (pp. 1-300) (New Zealand, Ministry of Social Development). Wellington.

The New Zealand Government, (2000). *Ministry reacts to James Whakaruru recommendations*. Retrieved April 30, 2016, from http://www.scoop.co.nz/stories/PA0006/S00570/ministry-reacts-to-james-whakaruru-recommendations.htm

PricewaterhouseCoopers New Zealand. (2016). *Exploring the big cyber questions A New Zealand context: Global State of Information Security Survey 2016*. Retrieved April 30, 2016, from http://www.pwc.co.nz/PWC.NZ/media/pdf-documents/pwc-security/pwc-global-state-of-information-security-survey-2016-exploring-the-big-cyber-questions-new-zealand-context.pdf

Privacy Commissioner. (2015). *Approved information sharing agreement: improving public services for vulnerable children.* A report by the Privacy Commissioner to the Minister of Social Development under section 96P of the Privacy Act 1993.

Case Note 202956 [2010] NZ PrivCmr 4: Woman complains about disclosure of transcript of meeting.

Small, V. (2013, June 11). CYF blackmailed after privacy breach. *The Dominion Post*. Retrieved April 29, 2016, from http://www.stuff.co.nz/national/politics/8782552/CYF-blackmailed-after-privacy-breach

Trevett, C. (2015, August 5). Adams tackles privacy paralysis: Information-sharing push for cases of domestic violence. *New Zealand Herald.* Retrieved April 29, 2016, from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11491957

APPENDICES

Appendix One: About Methodist Mission Southern (The Methodist Mission)

Organisational Background:

The Methodist Mission is a multi-disciplinary social service agency that has been operating throughout Dunedin and Otago since 1890.

The Methodist Mission's purpose statement is ***Change that Works: Enough Support and Challenge for you to Risk a Better Future.***

To achieve long-lasting, meaningful change in our clients, The Methodist Mission staff use high levels of skill, rigour and specialist tools; while paying attention and learning from what is discovered.

Model of Engagement: Our Process

The model of engagement is to move from ① a positive first point of contact ② to affirming the dignity of the people we work with ③ toward establishing a trusting and respectful relationship, ④ which supports the re-emergence of hope and aspirations ⑤ all while clearing away the clutter ⑥ toward the creation of transferrable resiliency, ⑦ enabling celebration at the achievement of goals ⑧ and finally, completion (and release) from service.

All programme delivery is directly aligned to The Methodist Mission's strategic vision by operating in a client-centred, strengths-based manner, to build resiliency and create sustainable long-term changes in the lives of clients.

People are empowered to use their existing skills and strengths, and The Methodist Mission staff work alongside them to provide the education, employment skills and specialist support services they need to achieve their goals.

Clients set their own goals and are responsible for achieving them. The Methodist Mission's job is to provide the specialist skills and support to remove their barriers to achievement and keep them on track.

The Methodist Mission works with clients so that they no longer need our assistance. Every service provided has an identifiable end point and builds client resiliency, so they are in a better place and are better equipped to deal with future issues, leading to meaningful, sustainable change.

All aspects of The Methodist Mission's work are heavily informed by best-practice research and analysis of The Methodist Mission's own client-derived data.

Current Programmes and Services
Programmes and services include:

- **Early Years Services Hub** - Free services for whanau with children aged 0-6 years.
- **Little Citizens Early Learning Centre** – Early childhood education for children aged 0-6 years.
- **Next Step Training** – Free foundation and second chance learning for youth and adults.
- **Corrections Programmes** – Educational and rehabilitative programmes for at prisons and Community Corrections sites throughout Otago and Southland.
- **Arahina Family Support Centre** – A wide range of social services for families in Mosgiel.
- **Client Support Services** – Specialist social work support for clients on a range of issues.
- **To Advocate** – A free independent advocacy service to enable social services, health and disability practitioners to obtain important information on behalf of their clients.
- **Beyond 10 Streets Community Development** – An innovative community development project in South Dunedin.
- **Research Projects** – Quantitative and qualitative research on a range of educational and social topics.

Appendix Two: Privacy principles. Privacy Act 1993, section 6.

Part 2

Information privacy principles

6 Information privacy principles

The information privacy principles are as follows:

Information privacy principles

Principle 1

Purpose of collection of personal information

Personal information shall not be collected by any agency unless—

(a) the information is collected for a lawful purpose connected with a function or activity of the agency; and

(b) the collection of the information is necessary for that purpose.

Principle 2

Source of personal information

(1) Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.

(2) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds,—

(a) that the information is publicly available information; or

(b) that the individual concerned authorises collection of the information from someone else; or

(c) that non-compliance would not prejudice the interests of the individual concerned; or

(d) that non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(e) that compliance would prejudice the purposes of the collection; or

(f) that compliance is not reasonably practicable in the circumstances of the particular case; or

(g) that the information—

(i) will not be used in a form in which the individual concerned is identified; or

(ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(h) that the collection of the information is in accordance with an authority granted under section 54.

Principle 3

Collection of information from subject

(1) Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of—

(a) the fact that the information is being collected; and

(b) the purpose for which the information is being collected; and

(c) the intended recipients of the information; and

(d) the name and address of—

(i) the agency that is collecting the information; and

(ii) the agency that will hold the information; and

(e) if the collection of the information is authorised or required by or under law,—

(i) the particular law by or under which the collection of the information is so authorised or required; and

(ii) whether or not the supply of the information by that individual is voluntary or mandatory; and

(f) the consequences (if any) for that individual if all or any part of the requested information is not provided; and

(g) the rights of access to, and correction of, personal information provided by these principles.

(2) The steps referred to in subclause (1) shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.

(3) An agency is not required to take the steps referred to in subclause (1) in relation to the collection of information from an individual if that agency has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.

(4) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds,—

(a) that non-compliance is authorised by the individual concerned; or

(b) that non-compliance would not prejudice the interests of the individual concerned; or

(c) that non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(d) that compliance would prejudice the purposes of the collection; or

(e) that compliance is not reasonably practicable in the circumstances of the particular case; or

(f) that the information—

(i) will not be used in a form in which the individual concerned is identified; or

(ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Principle 4

Manner of collection of personal information

Personal information shall not be collected by an agency—

(a) by unlawful means; or

(b) by means that, in the circumstances of the case,—

(i) are unfair; or

(ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 5

Storage and security of personal information

An agency that holds personal information shall ensure—

(a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—

(i) loss; and

(ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and

(iii) other misuse; and

(c) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

Principle 6

Access to personal information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled—

(a) to obtain from the agency confirmation of whether or not the agency holds such personal information; and

(b) to have access to that information.

(2) Where, in accordance with subclause (1)(b), an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.

(3) The application of this principle is subject to the provisions of Parts 4 and 5.

Principle 7

Correction of personal information

(1) Where an agency holds personal information, the individual concerned shall be entitled—

(a) to request correction of the information; and

(b) to request that there be attached to the information a statement of the correction sought but not made.

(2) An agency that holds personal information shall, if so requested by the individual concerned or on its own initiative, take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

(3) Where an agency that holds personal information is not willing to correct that information in accordance with a request by the individual concerned, the agency shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by that individual of the correction sought.

(4) Where the agency has taken steps under subclause (2) or subclause (3), the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

(5) Where an agency receives a request made pursuant to subclause (1), the agency shall inform the individual concerned of the action taken as a result of the request.

Principle 8

Accuracy, etc, of personal information to be checked before use

An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

Principle 9

Agency not to keep personal information for longer than necessary

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

Principle 10

Limits on use of personal information

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds,—

(a) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to use the information; or

(b that the use of the information for that other purpose is authorised by the individual concerned; or

(c) that non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; or

(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(d) that the use of the information for that other purpose is necessary to prevent or lessen a serious threat (as defined in section 2(1)) to—

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(e) that the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or

(f) that the information—

(i) is used in a form in which the individual concerned is not identified; or

(ii) is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(g) that the use of the information is in accordance with an authority granted under section 54.

Principle 11

Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,—

(a) that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or

(b) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information; or

(c) that the disclosure is to the individual concerned; or

(d) that the disclosure is authorised by the individual concerned; or

(e) that non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
(ii) for the enforcement of a law imposing a pecuniary penalty; or
(iii) for the protection of the public revenue; or
(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(f) that the disclosure of the information is necessary to prevent or lessen a serious threat (as defined in section 2(1)) to—
(i) public health or public safety; or
(ii) the life or health of the individual concerned or another individual; or

(g) that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or

(h) that the information—
(i) is to be used in a form in which the individual concerned is not identified; or
(ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) that the disclosure of the information is in accordance with an authority granted under section 54.

Principle 12

Unique identifiers

(1) An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any 1 or more of its functions efficiently.

(2) An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those 2 agencies are associated persons within the meaning of subpart YB of the Income Tax Act 2007.

(3) An agency that assigns unique identifiers to individuals shall take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.

(4) An agency shall not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.

Appendix Three: Unstructured responses to survey questions – practitioner survey[79]

Q: Are there any other barriers you face around sharing client information with other organisations?

- Differing cultural perspectives and practice
- Dodgy, corrupt organisations who hide behind the privacy act
- depends on the circumstances
- People not understanding the Privacy act properly and when they can share information.
- there arer still some organisations reluctant to shart specific information
- How much to share?
- In the NGO sector, it is always a concern that others do not handle such information up to standard.
- our consent to disclose form is ambiguous and confusing at best
- different electronic medical systems. urgent medical crisis and when lack of EPOA
- Different organisations and professions work differently. In my work as a [withheld to protect respondent anonymity] i do not find this much of a challenge because it all family led and if i have child protection concerns or mental health concerns i forward the info on and have always discussed it with family beforehsnd. I feel that if i could nit speak to them first and there were safety concerns i would still forward on. Main challenge is having an understanding of what happens next. Organisations are sometimes overly secretive rather than respecting confidentiality. I commonly find this when the practitioner is less experienced or confident in their role and are fearful of the structure and rules or do not have the time to manage a request for informstion professionally.
- Sometimes its essential to share information for the purposes of aligning multi-agency approaches and this is mostly not possible which is a shame because services fall short of meeting client needs.
- If the person (client) asks me not to and it is not a care and protection issue.
- When there are Mental Health, Safety issues
- Education providers have very different understanding of what can and cannot be share - clients sign a disclosure form permitting information collection for benefit purposes
- I know I can share information but it is always an inconsistency about the level of information and where my responsibility ends .
- Other organisations have withheld information about a client who poses a threat to others eg physical/safety concerns. I work in youth education and we have a duty of care for the young people we work with. If we know of a safety concern we can put plans in place to support all parties concerned
- Practitioners unwilling to share as they fear it may comprimise their relationship with the client, even when safety is of concern.

[79] Responses are verbatim unless identifying comments were made in which case these were removed.

- Expectations of other organisations wanting information right then and there. Then asking that same organisation for information and being told to write a request and given a timeframe.
- Interagency info sharing

Q: Please add any comments should you wish to do so

- We are also well school, because of our training, on when we can share information without the consent of our clients and made them aware of this at the first point of contact with our agency. New staff members than myself may be less confident, and more likely to consult managers/colleagues.
- depends upon the given circumstancs at the time. every case is different.
- We have a "privacy policy" but I don't recall having any formal training on how to apply this, and it is difficult to remember the principles and subsequently apply them during a busy day at work.
- there is a difference between formal and informal sharing of information
- Some of the questions I have answered e.g. something about putting request in writing and there was another comment here to...something about recording the request in writing I think,...I will always document in the case notes the consent and whom the information was provided by. There was another question about gaining info without consent - not sure if it was worded very well - consent is not needed if risk / safety issues are of concern for example I will inform a parent or caregiver if I am making a report of concern to CYFS, but I don't need their consent to do the report of concern...
- Re questions 22 and 23. if a client requests information we discuss with our manager and go through certain channels, however requests from other organisations are not treated this way.
- I am lucky to be working for an organisation that has very clear guidelines around this Act and we have good back up when we are in doubt.
- I think there is more room in the health sector for further sharing?
- Privacy Act matters are a very good thing and a barrier. It would be useful if barriers to sharing information could be overcome for the purposes of multi-agency approaches to problem solving.
- Sharing someones information always feels like there are a lot of grey areas. It is still someones private information in the issue of safety I have now concerns but with assisting someone to get the benefits they may need due to a disability or injury that feels like the hardest area to walk through.

Appendix Four: Unstructured responses to survey questions – manager survey

Context: Do staff members who have access to client information receive training/instruction on how to use the principles of the Privacy Act 1993 in their practice?

Q: How does this training take place? (Select all that apply): Other

- received at orientation then ad hoc at PD days
- online evidence based learning
- I (Manager) am a fully trained privacy advocate and also deliver education outside of our organisation to other NGOs on privacy
- often included in external training programmes eg Uni,Polytech etc
- We have got a privacy code tool kit
- Through manager meetings and audit processes
- Informal colleague discussions
- part of induction
- By our National Training Unit

Context: Does your organisation require staff to explain to clients for what purpose they are collecting the client's information and how this will be used and stored?

Q: How is this explanation conveyed to the client? (Select all that apply): Other

- Have got poster up in waiting room and pamphlets available to clients about collecting information.
- through whanau pani

Q: Who has your organisation had requests for client information from? (Select all that apply): Other

- Lawyers Custodial Parents
- lawyers acting for the child, Police
- lawyers on behalf of clients, Police, CYF Service
- Lawyers
- Family
- Insurance companies, other legal organisations
- other clients
- others
- Lawyers, GPs,other district health boards in New Zealand and overseas
- Lawyer for children/parents
- parent
- The client's family, lawyer and creditors. Also Police
- Lawyers

- Parent or Whanau member

Context: Do staff members receive instruction/training on how to ensure compliance with your organisation's Approved Information Sharing Agreement?

Q: How does this training take place? (Select all that apply): Other

- Individual and induction training
- National Training Unit / Privacy and Official Information Team based in Wellington
- client reveiws
- Staff must read and be aware of the Privacy Act as it relates to their working relationship
- Orientation

Context: Are staff members trained/instructed on what steps to take if they determine that there will be an adverse action to a client if the client's personal information is shared?)

Q: How does this training take place? (Select all that apply): Other

- clinical manager will also discuss on a one to one with Staff

Q: Please add any comments should you wish to do so

- Clients are often surprised they are not required to sign that they have received info about storage/sharing of information.
- I recently explored the Privacy Act related to storage of information for clients who had exited services and found the information provided on the web site was quite conflictual
- We have a very tight regime regarding personal information we hold on clients, staff, volunteers and our organisation in general.
- We are a new organisation that is in the process of creating policies as well as being part of a National Body that is also in the process of creating national policies.
- We as an organisation are extremely careful and respectful of private information
- We are a small youth service with two staff. All information stored on clients is on a password protected computer that only the two staff members have access to.
- Information sharing guidelines are adhered to and are part of Continous Quality Improvement (CQI) and safe ethical practice.
- Some agencies and organistations are not always clear about the provisions and protections under the Privacy Act around disclosure of information when it relates to the Care and Protection of children and young people.