TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

Chair in e-Government

Emerging Issues Programme Research Project Report

'Improving Information Sharing for Effective Social Outcomes'

Professor Miriam Lips, Dr Rose O'Neill[1] and Elizabeth Eppel

Victoria University of Wellington
December 2009

[1] Dr Rose O'Neill's contribution is based on her research involvement as a Research Fellow until 22 July 2009, and only reflects the personal views of the author

Contents

1. Introduction

In order to build government structures and activities more around the fundamental needs of individuals and to achieve more effective social outcomes for New Zealanders, how can cross-government information sharing be improved, taking into account fundamental rights like the privacy protection of individuals? What can be learned from other jurisdictions in that respect? These questions have been examined in a project commissioned by Public Service Chief Executives under the Emerging Issues Programme (EIP) based on a partnership between VUW's School of Government and the Public Service. The project was coordinated by Dr Miriam Lips, Professor of e-Government at VUW. The research took place from September 2008 until October 2009.

Focus of the research

Transforming service design with a primary objective to achieve effective social outcomes is one of the key challenges for public management in the 21st Century. Vulnerable individuals and families dependent on welfare support (i.e. individuals and families at risk, such as long-term unemployed, homeless, refugees, youth offenders) often are facing complex problems with interrelated, underlying causes located in various policy domains, such as unemployment, education, health, housing, and justice. Traditionally, it is expected that these individuals join up the existing structures of government in a way that the complexity of their problems can be met. By taking a more holistic viewpoint of individuals' needs however, increased effectiveness of public service provision can be achieved by building government support around those interrelated needs of the individual or family at risk. Using an integrated service response approach of 'no wrong door', the New Zealand Ministry of Social Development together with several government and non-government organisations, already is working towards transformed public service design in order to achieve more effective social outcomes.

To support this paradigm shift of organisation-centric to citizen-centric government, improving information sharing across government is essential and Information and Communication Technologies (ICTs) are therefore critical infrastructure of 21st Century government. Internationally however we can observe that the introduction and use of ICTs can have a huge and varying impact on the ways in which personal information of individuals or families is handled across the public sector, ranging from increased levels of information security to increased risks of large-scale data breaches. With substantial, ICT-enabled changes to public service design being considered, including increasing information sharing across government, emerging tensions around the safeguarding of fundamental citizens' rights, such as privacy and confidentiality, need to be taken into account (Bellamy *et al*. 2005; 6 *et al.* 2005).

Countries with similar jurisdictions to New Zealand, such as the UK, Canada and Australia, are developing strategies to overcome these tensions between goals of service transformation and the privacy protection of individuals, with a current focus on allowing specific information sharing arrangements for targeted user groups, such as children or the most disadvantaged in society, and developing cross-government Identity Management (IDM) solutions. Some overseas policy makers even seem to believe that privacy legislation is standing in the way of progress towards improved information sharing that will support the transformation of public service provision. On the other hand, on the basis of an independent review of the UK Data Protecton Act and policy relating to data sharing in the UK, Thomas & Walport come to the conclusion that, "*in the vast majority of cases, the law itself does not provide a barrier to the sharing of personal data. However, the complexity of the law, amplified by a plethora of guidance, leaves those who may wish to share data in a fog of confusion*" (Thomas & Walport 2008, p.i).

Nationally and internationally so far however, there is a lack of empirical research on information sharing practices of government agencies, including the role and implementation of privacy legislation. Consequently, the focus of this research was to empirically examine information sharing practices between agencies in New Zealand, and more specifically in areas where public officials are dealing with multiple, fundamental problems from the viewpoint of the individual or family, such as combined problems of unemployment, poor education, health, housing, and crime. Usually, these complex problems are at the interface of various policy domains (e.g. social, economic and justice) and multiple government and other organisations (e.g. Ministry of Social Development, NZ Police, Probations, Health, Refugees' services organisation, Auckland City Council). This project has been further scoped to empirically explore case studies of individuals and families at risk (or imminent risk).

Key objectives and research design

The objective of this project was to identify opportunities for improved information sharing across the NZ government in order to achieve more effective social outcomes, without compromising fundamental rights of individuals, such as privacy protection and confidentiality.

In order to achieve that objective the research first needed to empirically explore to what extent and how personal information related to complex, multiple needs of individuals or families in the wider social policy area (including health, education and justice) is collected, managed, and shared in a variety of joint service arrangements across government and other organisations involved. This research activity involved qualitative research including a wide variety of case studies. Secondly, in order to identify potential learning opportunities for improved information sharing from jurisdictions overseas, a document study was conducted of existing strategies and arrangements for cross-government information sharing in the UK, Canada and Australia. Research findings from both activities have been discussed and further developed in three solutions-oriented focus group meetings with front line staff members, middle managers and other experts in the area of cross-government information sharing, and in feedback sessions with research participants.

The research project focused on the following questions:

> *To what extent and how is personal information of individuals with complex social needs collected, managed, and shared across government and other organisations?*
>
> *What are barriers and enablers to cross-government information sharing?*
>
> *What are existing strategies and arrangements for enabling cross-government information sharing in other jurisdictions? What can New Zealand learn from other jurisdictions in that respect?*
>
> *How, and under what conditions, can cross-government information sharing be improved in order to achieve more effective social outcomes?*

Furthermore, a reference group was established for this research project, which included representatives of stakeholder organisations, such as the Ministry of Social Development, Ministry of Justice, NZ Police, Department of Corrections, Ministry of Women's Affairs, State Services Commission, Treasury, the Office of the Privacy Commissioner and the Office of the Ombudsmen.

Overview of this report

First of all, in chapter 2 of this report, we present an overview of available academic literature in the field of cross-agency collaboration and information sharing, with a specific focus on New Zealand-based research. We used this literature review to develop a theoretical lens on the basis of which we explored our empirical research object. In chapter 3, we describe the research design of this project, including the research methodology and criteria used for the selection of case studies. The case study findings are presented in chapter 4; this chapter is organised around five different cross-agency initiatives that were selected for the research. Several of these included more than one location, making up the eight cases included overall in the research.

A cross-case study analysis of the research findings is provided in chapter 5. In chapter 6, we report on information sharing approaches and solutions adopted in the United Kingdom, Canada and Australia, and briefly point out the main differences compared to the New Zealand research findings. And finally in chapter 7, based on the research findings, we present solutions and recommendations for improving information sharing to establish effective social outcomes in New Zealand.

2. Available literature on cross-agency collaboration and information sharing

Information sharing across public sector organisations and their NGO partners takes place in a public management context involving people from multiple government and non-government organisations. Horizontal arrangements between different organisations are referred to as 'networks' in the scholarly literature. Networks are often juxtaposed to hierarchies, and markets, although many researchers point out that it is not a case of 'either – or', but 'and'. Horizontal approaches to improve the delivery of public services have been referred to as 'joined-up government'. Thus this chapter briefly summarises the scholarly literature on networks and joined-up government canvassed in an earlier review (Eppel 2007) and with a specific focus on New Zealand-based research. Furthermore, this chapter seeks to integrate other scholarly research, particularly where information sharing and processing of personal information on the citizen is at the heart of the joined-up effort. At the end of this chapter, a brief overview is provided of the specific legal context for cross-agency information sharing in New Zealand, the Privacy Act, 1993.

Joined-up government

The idea of 'joined-up government (JUG; also called 'collaborative' or 'integrated' government) has been practiced and researched within a number of international jurisdictions including the UK, Netherlands, USA, Australia, Canada and New Zealand, as a response to fragmented and non citizen-focused delivery of public services.

In a New Zealand-based research project conducted under the Emerging Issues Programme in 2007 and 2008, seven examples of joined-up government were investigated (Eppel *et al.* 2008). The findings from this project have been analysed in comparison with available international research findings about: when and why joining-up across government is a good idea; how joining up happens – what helps and hinders joining-up. These are summarised in turn in the following sections.

Why and when to join-up

In many cases, joining-up across organisations is a response to two problems. The first problem is a structural one relating to the bounded focus of each organisation and the tendency for government services in New Zealand and elsewhere under what has been branded 'New Public Management' to be delivered by single focus organisations or contracted, third-party organisations (6 2004).

The second problem is that, as citizen needs for services become more complex, the services they require are likely to be spread across the ambit of a number of government agencies. The more fragmented and multi-causal the issues faced by citizens, then the more difficult it is for any government agency, or service delivery organisation, to understand the problem, and deliver appropriate, high quality services focused on the client's needs.

The efforts of government agencies to work together can result in a continuum of degrees of joined-up government summarised in Figure 1. They can range from informal, ad-hoc arrangements and information exchanges, to formalised, shared working initiatives on integrated service delivery.

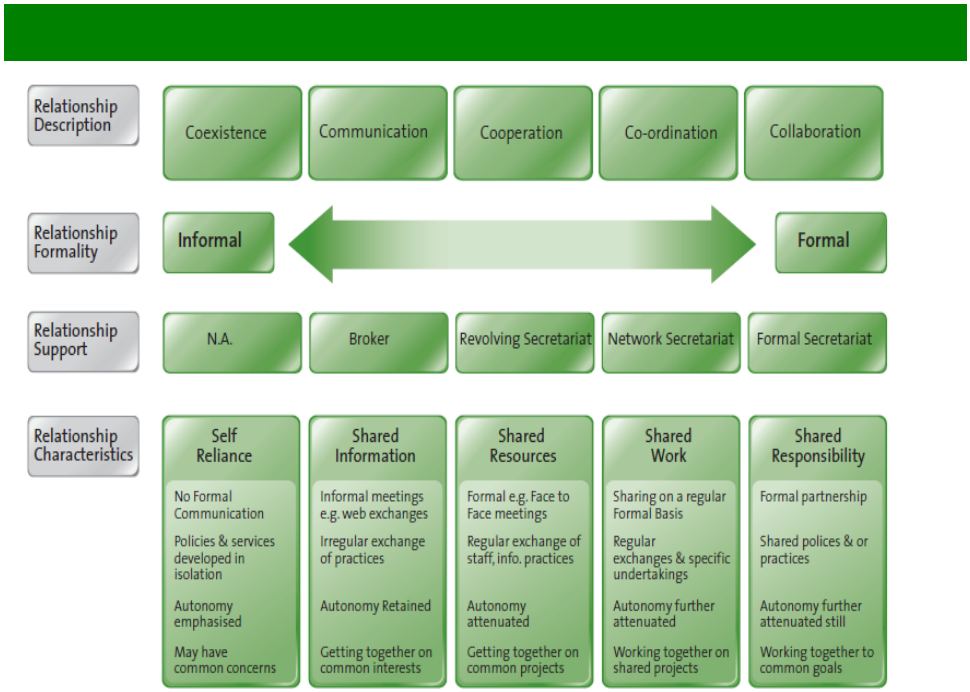

Figure 1 Continuum of inter-agency integration

There is no right answer to the question what is the appropriate level of joining-up (6 2004). Working across different agencies and joining-up is not easy, and takes time and additional effort by the individuals and agencies involved. However when the issues being dealt with are complex, fragmented and multi-causal, then it is more likely that no one agency has sufficient information or resources to address the issues alone (Conklin 2006; Ritter & Webber 1973). A general rule is that the complexity of the public management response needs to match the complexity of the problem. That is, the more the clients' needs are complex and need to be addressed by multiple agencies, the more government agencies need to move towards the collaborative end of the continuum to address their information and resource deficiencies (Bryson *et al*. 2006; Klijn 1997).

The New Zealand research identified two critical factors that influenced a decision by agencies to join-up in a more collaborative, problem sharing and problem solving way. The first is a so-called "ah-ha moment": the recognition by one or more people that the issue, or problem, cannot be dealt with in the normal way – that the agencies' usual way of doing business and standard procedures are inadequate for the circumstances.

The second critical factor identified in the research is a trio of roles with particular characteristics: the roles of the so-called 'public entrepreneur', 'fellow-travellers' and 'guardian angels'. These roles are not limited to a single person but all three of these roles are necessary to take a 'ah-ha' moment and turn the handling of an issue into a successful inter-agency collaboration.

The 'public entrepreneur' is the individual(s) who takes that moment of recognition that an issue 'doesn't make sense' or 'this does not fit within our standard ways of working' or 'we don't have enough information or resources to deal with this issue' and begins to seek out other people – 'fellow travellers' – like-minded people in other agencies who might have a part of the information needed to understand the issue and find a solution.

Most incipient collaborations of this sort will not come to much, unless there are so-called 'guardian angels', that is, people who can act as critical friends, mentors or protectors, to allow a new way of working to develop.

Ways to join up

The style and specifics of interagency working are highly contingent on the specific context, issues to be solved, and the people involved; however, the literature does offer some guidance about what needs to happen to support cross-agency working. First of all, because of the fragmented and difficult to define nature of some public management problems, and the existence of many perspectives on their causes and solutions, a culture of learning is needed. This includes learning from the perspective and experiences of others, as well as learning by doing. Complex problems do not lend themselves to simple solutions. However, they can be addressed by an iterative process of assessment, learning, acting, re-assessment, learning and further action.

Joining-up goes through a series of phases following the 'ah-ha' moment that acts as the trigger for doing things differently. The New Zealand research characterised these phases as 'before starting', 'getting together', 'working together', and 'sustaining' (see Figure 2). It also noted the importance of the culture of leaning from others and learning from doing, and the need for support from 'home' organisations for the collaborative processes.

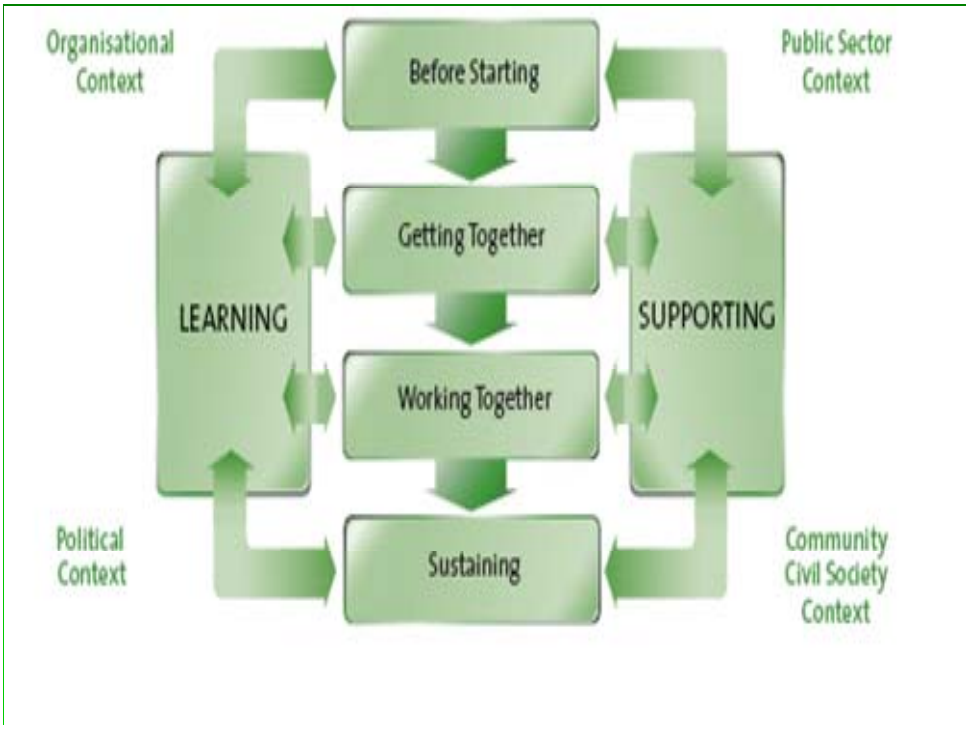

Figure 2 Phases of Joining-up

Joining-up and information sharing between organisations is affected by the context in which it takes place (Bryson *et al.* 2006; Crosby & Bryson 2005; Eppel *et al*. 2008; Ryan *et al*. 2008). The following contexts are relevant:

- public sector context;
- political context;

- organisational context; and
- community context

The public sector context implies that attention must be paid to the 'authorising environment' which influences what services need to be delivered and how they are delivered (Moore 1995).

The political context is part of the authorising environment. The management of public policy problems and delivery of public services cannot be completely at variance with political priorities and directions. The New Zealand research examples suggest that some activity remains 'beneath the radar' because of uncertainty about political acceptability and authorisation. In these circumstances the role of 'guardian angels' becomes critically important in creating alignment between the joined-up activity and political context.

According to 6 *et al*. (2006), the nature and form of the organisations involved in joining-up affects the nature and form of the collaboration. Strong hierarchical organisations are likely to be more rule-bound, procedurally wedded to their organisational ways of working. They are more likely to be intolerant of entrepreneurial ways of working which are independent of formal position of the individuals involved.

The community context will also affect the nature of the collaboration and the extent to which people in the community of clients can be involved in the horizontal processes of problem identification and problem solution. Bearing in mind that no one organisation has sufficient information or resources to address issues alone, community and client perspectives could be vital to ensuring the right services are available and that service quality is fitted to needs.

Working together

Agranoff and McGuire (2001) posit that there is a set of management behaviours and responsibilities associated with horizontal network management different from and parallel to the traditionally acknowledged 'POSDCORB' framework (i.e. Planning, Organising, Staffing, Directing, Co-ordinating, Reporting, Budgeting) (Gulick & Urwick 1937). These behaviours and responsibilities include:

- 'activation' – identifying participants in the network and tapping their skills, knowledge and resources: network managers arrange, stabilise as much as possible, nurture and integrate the network structure;
- 'framing' – occurs during formation and operation of the network and involves establishing and influencing the operating rules of the network, influencing its prevailing values and norms, and altering the perceptions of the network participants;
- 'mobilising' – requires a view of the strategic whole: network managers must induce individuals to make a commitment to the joint undertaking and to keep that commitment; they must mobilise organisations and forge agreement on the role and scope of network operations, which involves motivating, inspiring and inducing commitment; and
- 'synthesising' – creating the environment and enhancing conditions for favourable, productive interaction: network managers must find a way to blend the various participants, each with conflicting goals or different perceptions or dissimilar values, to fulfil the strategic purpose of the network (Mandell 1999).

Network leadership

In a horizontal, inter-organisational network the key behaviours and responsibilities fall on the collaborative group of individuals; each group must arrive at an accommodation for how these responsibilities will be shared. This has implications for the leadership appropriate in these networks. Huxham & Vangen (2000) refer to this as the shaping and implementing of collaborative agendas, which is affected by the network structure and its member organisations. Depending on the structure of the network, some leadership may come from outside of the formal membership of the network, e.g. the CEO of one of the member organisations.

Networks are in effect a type of loosely coupled organisation, different from the traditional vertical organisation and they require different leadership skills. Mandell (1999), Kickert *et al.* (1997); Agranoff & McGuire (2001) all stress that managing in inter-organisational arrangements is different from the vertical and horizontal management that goes on in organisations.

Different skills and knowledge are needed for cross-agency collaboration. Compared with the conventional hierarchical organisation there is no central authority; therefore, facilitative leadership, rather than one based on command and control, is needed. The focus is on selecting appropriate actors and resources, shaping the operating context and developing ways to cope with the strategic and operational complexity (Agranoff & McGuire 1999). Rather than controlling, the focus needs to be on co-ordinating the strategies of actors with different goals and preferences with regard to a certain problem or policy measures, within an existing network of inter-organisational relations (Kickert, *et al*. 1997, pp. 10-11). Crosby & Bryson (2005) conclude that the 'potential for effective leadership lies alike with those who do and do not have formal positions of power and authority' and power and influence remain concentrated in certain 'nodes' of leadership who lead 'up and out rather than down'.

Many scholars have identified the achievement of goal consensus and trust as essential outcomes of effective leadership for working together across organisations. Hudson (2004) says that the effective operation of a network requires that its different participants are clear about the roles and responsibilities to be undertaken by themselves and other members. This will be affected by the extent to which network members have an understanding of their inter-dependence which is the fundamental basis for their collaborative problem-solving efforts.

Goal consensus

Achieving goal consensus is not the same as doing everything together and agreeing on everything. But it does mean achieving broad agreement on the overall outcome the horizontal group is trying to achieve. This type of consensus is more likely where organisations have similar goals. Relationships among organisations that may have similarities but operate in different sectors can be intense and stable in nature. In contrast, where organisations of the same kind are producing the same product or service, relationships are predicted to be fragile and insecure, and domain consensus can be predicted to be difficult to achieve (Hudson 2004).

Hudson (2004) also notes that there are two levels of ties that may link partners together: ties at an institutional (or policy) level usually conceptualised as organisational forms; and ties at a more micro-analytic, transactional level (provider networks). Together they form a basis for thinking about the nature of 'whole systems' working that is urged upon service commissioners and providers. The literature on inter-organisational networking has tended to conceptualize the ties linking organisations at the rather aggregate level of organizational forms. What is

now needed, says Hudson, is a better understanding of some lower-level ties – the characteristics, intentions, aspirations or situation of participating actors – at the level of provider networks. This was also confirmed by the New Zealand study which identified the need for linkages at the top/policy level of the organisations and at the service delivery/front line, but also in the middle to help forge consistent ways of supporting the collaboration across the organisations involved.

Hudson (2004) and the New Zealand study (Eppel *et al.* 2008) both emphasise the dynamic nature of the inter-organisational relationship and the policy problems they are addressing. It is a dynamic framework capable of capturing change, and one that makes no assumptions about a specific plan, network 'cycle' or journey. Evaluation, review, learning and reassessment need to be part of a continuous process undertaken within the horizontal 'organisation' and with support and interaction from the vertical organisations involved.

Trust

A critical ingredient of successful cross-agency working identified by nearly all studies is trust. Perri 6 *et al*. (2006) provide an extensive discussion of the concept of trust between organisations. They offer the idea of trust being linked to a task: for example, an organisation's statistics might be trusted while some other aspect of their performance, such as follow through on complaints, might not. Trust relates to the expectations of others. It can also be seen as linked to the willingness to play according to accepted rules.

Rommel and Christiaens (2009) point out that by co-ordinating the actions of actors, trust allows actors to co-operate. High trust is assumed to result in a deeper form of collaborative behaviour between partners. Partners that trust each other will engage in increased information-sharing, especially the sharing of tacit information (Edelenbos & Klijn 2007). They will also share strategically important information and competencies, allowing the partner to learn and to innovate. Furthermore, partners will engage in joint problem-solving and joint action (Dyer & Chu 2003; Muthusamy & White 2005). High trust will reduce the need for control, so that transaction costs and the need for formal contracting are reduced (Ring & Van de Ven 1992; Das & Teng 2001).

Hudson (2004) summarises the benefits for inter-organisational working and outcomes arising from trust. Sharing of values characteristic of trust promotes several kinds of social processes leading to the development of 'synergistic team relationships' in an organisational setting and, with that, to superior performance. These include:

Broad role definitions*:*

> How broadly or narrowly individuals define their work roles has been shown to influence co-operative behaviours. When conditional trust exists, individuals define their roles in accordance with expected job behaviours and assigned duties; with unconditional trust, the interactions are likely to lead individuals to define their roles more broadly.

Communal relationships*:*

> The shared values underlying unconditional trust guide people to strive for communal relationships characterized by helpfulness and responsibility, and to contribute to the development of such relationships. Communal relationships, in turn, are likely to promote inter-personal co-operation and teamwork.

High confidence in others*:*

> The shared values that underlie unconditional trust provide individuals with the high degree of confidence in each other necessary for synergistic team relationships to emerge, because one can be assured of others' ultimate intentions and objectives.

Help-seeking behaviour*:*

> Seeking help is not threatening under unconditional trust because inter-dependence is seen as a positive force, and shared values and positive attitudes ensure against attributions of inadequacy.

Free exchange of knowledge and information*:*

> Knowledge and information are not likely to be exchanged freely when one party cannot be sure about the moral basis of another party's actions or the values that are prospectively guiding that party's behaviour. However, with unconditional trust, the underpinning shared values provide individuals with the assurance that knowledge and information will be used for the wider good.

What hinders joining-up

The previous sections have identified what is needed to make horizontal, inter-organisations ways of working successful. Conversely failure to have regard to these matters will place the arrangement at risk. The New Zealand joined-up government research findings suggest that sustaining a cross-agency way of working requires support and understanding of the practicalities encountered when working horizontally as well as of the importance of developing accountability and review processes suited to this way of working. Such arrangements most often fail or cease to work effectively because home organisations withdraw their support or because one organisation imposes its organisational requirements on the inter-organisational arrangement.

Information sharing across organisations

Increasingly, in many countries around the world, improving cross-agency information sharing to enhance the quality of public services to individuals, especially those at risk, such as children, the sick and elderly, homeless, youth criminals, long-term unemployed, refugees and others with high and complex needs is at the heart of public management reform efforts (e.g. 6 *et al*. 2005; Varney 2006). Often, these reform efforts are further supported by the publication of model information-sharing protocols designed to promote increased sharing of client information across agencies, and the roll-out of ICT infrastructures and systems to promote cross-agency information sharing (e.g. Bellamy *et al.* 2008).

More in general, the capabilities of ICTs to facilitate cross-agency information sharing and integrate public sector information in networked environments have been widely acknowledged. Perceived benefits are increased productivity, improved decision making, the reduction of administrative burden (e.g. duplication), better law enforcement, higher information quality (resulting in fewer mistakes), and integrated services (Gil-Garcia *et al.* 2009, p.1). However, cross-agency information sharing and integration is also perceived as a difficult and complex activity, with important barriers in technical (e.g. incompatibility of

hardware and software, data incompatibility), organisational (e.g. diversity in organisational cultures, conflicting organisational priorities, lack of funding), political (e.g. lack of political support), and legal domains (e.g. restrictive laws and regulations) (Gil-Garcia *et al.* 2009, p.3–4).

So far however, there is not much empirical research available on how various government and non-government agencies are handling the sharing of clients' personal details in the establishment of cross-agency collaborations. Available research findings in this area indicate that there are many cases where information is still not shared when it should be, or where it is shared when it should not be (Bellamy *et al*. 2008, p.737). In the last decade, these research findings usually have been confirmed by dedicated research into information sharing practices around terrorist attacks and the protection of national or homeland security, leading to scholarly observations that, in many countries, policy discussions about the collection and sharing of personal information across agencies, as well as resulting actions around and regulations of information privacy, have taken on a different character (e.g. Regan 2004; Roberts 2004; Gellman 2004). Similarly, other recent societal 'crises' involving cross-agency information sharing, such as Hurricane Katrina in the USA or the Victoria Climbie murder case in the UK, appear to have opened up policy discussions around the information sharing failings of government agencies and urged for substantial changes to existing institutional arrangements, such as the creation of new legislation, changes to governance structures and leadership of government agencies, and the introduction of new information systems (e.g. Wetmore 2007; Bertot & Jaeger 2007; Peckover *et al.* 2008).

Gellman (2004) points at the phenomenon of 'mission creep' as a potential outcome of the introduction of new personal information systems: the development of secondary or tertiary uses of these systems far beyond their original purpose. As an example, Gellman raises the mission creep of the Social Security Number (SSN) in the USA, which started life in the 1930s with a simple purpose expressly unrelated to identification, and eventually became an all-purpose identification number, with dozens of legally authorised uses, and an untold number of unregulated uses (Gellman 2004, p. 499). Gellman also points at the potential development of 'database derivative activities': activities ancillary to the original purpose for which a database of personal information was compiled. These ancillary activities occur within the same plane as the original purpose as direct extensions or derivatives of that purpose undertaken by the operator of the database or by somebody else (Gellman 2004, p. 500). For example, in the USA, the history of the credit reporting system demonstrates a large variety of derivative activities, such as instant credit support, identity theft and identity theft assurance, credit watch services, and credit scoring and rescoring (Ibid).

One of the few empirical research projects on cross-agency information sharing reported in the literature looked at eight multi-agency arrangements in the UK, situated within policy domains of integrated health and social care, crime reduction, and public protection, in which personal information of individuals at risk is being shared (Bellamy *et al.* 2008; Bellamy *et al*. 2007) The research findings demonstrate that consistency of information sharing is dependent on how discretion is exercised in the street-level management of individual cases. As information sharing decisions often need to be taken in the absence of decision rules that would be obvious and acceptable to all interested parties, professional workers face continual dilemmas between the risk of 'false negative' error judgements (i.e. when no action is taken, but where it turns out later that it should have been taken) and the risk of 'false positive' judgements (i.e. where action is taken, although it turns out later that the risk was lower than would justify it) (Bellamy *et al*. 2005, p. 51).

The research findings further show that, with top down political pressure and prescription, information sharing practice is patchy, even within the same organisation. Generally, the people involved in these arrangements showed greater confidence that confidentiality would be respected appropriately, than that information would be shared appropriately. The researchers observed that informal 'work-arounds' were used to address gaps, deal with inconsistencies and reduce bureaucratic transaction costs (Bellamy *et al*. 2008, p. 753). The overall conclusion of the research was that deficits in social integration of public officials in cross-agency partnerships, as well as deficits in formal regulation, are significant in inhibiting the development of consistent and appropriate information-sharing practices. Where the volume of information-sharing is increasing, this may be as much the result of instrumental, individualistic and coping behaviours as of an increase in formal regulation (Bellamy *et al*. 2008, p. 757).

The New Zealand legal context for cross-agency information sharing: the Privacy Act, 1993

The Privacy Act, 1993, has as one of its main purposes the promotion and protection of individual privacy, in accordance with the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The Act is primarily concerned with good personal information handling practices and, with few exceptions, applies across the public and private sectors in New Zealand. According to the Act, 'personal information' means information about a living human being: the information needs to identify that person, or be capable of identifying that person.

The Act contains twelve information privacy principles dealing with collecting, holding, use and disclosure of personal information and assigning unique identifiers, such as IRD numbers or driver's licence and passport numbers. A frequently mentioned privacy principle by research participants in this research project is information privacy principle eleven[2] (especially 11(f)), as follows:

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; 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

[2] http://www.privacy.org.nz/privacy-principle-eleven/

(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 and imminent threat 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.

Furthermore, the Act gives the Privacy Commissioner the power to issue codes of practice that become part of the law. These codes may modify the operation of the Act for specific industries, agencies, activities or types of personal information (e.g. health information).

3. Research Design

In this chapter we further introduce the research methodology used in this study. Furthermore, we present the selection criteria used to identify potential case studies and explain how we came to our final selection of five case study areas out of an initial selection group of twenty programmes.

Research methodology

The overall purpose of this project was to identify opportunities for improved information sharing across government agencies and other organisations in order to achieve more effective social outcomes with regard to individuals or families at risk (or imminent risk). To be able to identify opportunities for improved cross-government information sharing we first of all needed to have an empirical understanding of information sharing practices between agencies in areas where public officials are dealing with multiple, fundamental problems from the viewpoint of the individual or family, such as combined problems of unemployment, poor education, health, housing, and crime. Moreover, we sought further empirical understanding of barriers and enablers of cross-government information sharing, which we then could use to identify opportunities for improved information sharing.

Acknowledging a lack of empirical knowledge on the extent, forms and ways in which New Zealand government agencies and other organisations are sharing information on vulnerable individuals or families with complex social needs, we used a qualitative case study research method to empirically explore multiple cross-government initiatives selected on the basis of a predefined set of criteria (Appendix 1). Within five cross-government programmes, of which three had information sharing protocols in place, eight qualitative case studies were conducted between January 2009 and May 2009, involving approximately 70 interviews with professionals.

Based on available literature in the area of cross-government collaboration and information-sharing (see chapter 2), a set of analytical themes was constructed to explore information sharing practices, applied procedures, perceived barriers to information sharing and perceived enablers. For instance, themes included ‘relationships with partner organisations’, ‘relationships with other professionals’, ‘ways of working’, ‘interpretation of information sharing procedures’, ‘experience with information sharing arrangement’, ‘types of personal information collected and managed’, ‘treatment of sensitive information’, and ‘availability and use of ICT-infrastructures/applications’. These themes were used in semi-structured interviews with front-line staff members, middle management, and senior staff involved in the eight case studies. Empirical data collected in the case studies was further tested and developed in three focus group meetings with public officials, academics, and legal experts: two focus group meetings took place in Wellington on 20 July 2009, and one in Christchurch on 22 July 2009. Furthermore, the empirical research findings were further discussed in feedback sessions with research participants in Hawke’s Bay on 26 August 2009 and in Auckland on 9 September 2009.

Case study selection criteria and assessment

Based on available literature, and considering the need to explore a wide variety of information sharing practices and experiences, including successful and less successful practices and experiences, the following variables were specified for identifying the case studies most suitable for inclusion:

- Focused on individuals or families at risk (or imminent risk);
- Complex, fundamental (so-called "wicked") problems at the intersection of multiple policy domains (e.g. social, economic and justice; social, education and health);
- Multi-agency engagement, such as crime, health, housing, income support, welfare and education;
- Varying partner arrangements (e.g. including local government, NGOs, private sector);
- Varying coordination arrangements in cross-government initiatives;
- Established ways of working between organisations (rather than new initiatives or concepts);
- Initiatives are currently operational;
- Regional spread of case studies (e.g. urban/rural/metropolitan; South / North Island);
- Sensitivity of personal information being shared (e.g. health, crime-related information);
- Varying information sharing arrangements under the Privacy Act, 1993 (e.g. information sharing protocol, Code of Practice, special information sharing regime for the Police; no specific information sharing arrangement);
- Varying characteristics of individuals/or families participating in public service design (e.g. active vs. passive case management of 'participants'; state-dependent vs. independent; voluntary vs. obligatory participation; age);
- Different ethnic groups, including Pakeha, Maori, Pacific Islanders, Chinese and other migrants;
- Variety of available ICT infrastructure, applications, skills and knowledge within and across agencies and other organisations involved.

To identify potential case studies, a number of public officials were contacted for information about current initiatives that involved inter-agency information sharing to deal with individuals or families with complex needs. Agencies consulted include the Ministry of Social Development; NZ Police; Ministry of Justice; Department of Corrections; Office for Older People, Funding and Community; Office of the Privacy Commissioner; Office of the Ombudsmen; Ministry of Women's Affairs; Ministry of Education; and the Ministry of Health.

The following selection group of twenty programmes was considered for inclusion in the research project:

(1) Priority offenders' initiative
(2) Offender reintegration project
(3) Joint initiative for employment outcomes for prisoners
(4) High Risk Offenders
(5) High Risk/ High Profile Forums
(6) Iwi crime prevention plans
(7) Supported bail
(8) EMBAIL - Electronic Monitoring Bail
(9) Drug & Alcohol Services
(10) ENROL – tracking students through the education system
(11) Family Violence Responses
(12) Foreshore and seabed
(13) Family Safety Teams
(14) ENLIVEN – home based support to older people
(15) Multicultural Service Centre for Refugees

(16) Community with Muslim Women in Auckland
(17) Strong Pacific Families
(18) Elder Neglect & Abuse Prevention Services
(19) DHB/ Police initiative in the area of missing people with mental health problems
(20) Integrated Service Response

On the basis of the selection criteria presented above, the initial selection group of twenty programmes was assessed as follows:

Complex problem interface

Of the options considered, some of the initiatives did not meet criteria of dealing with 'wicked' problems relating to social interfaces: tracking students through the education system (10) and issues relating to foreshore and seabed (12). Some of the initiatives that did meet this criterion were not yet established programmes (or pilots). These included the iwi crime prevention (6) and supported bail (7) initiatives. In addition, insufficient information was gathered on the initiative with Muslim women in Auckland (16). As other initiatives in the selection group dealt with migrant issues, this initiative was not considered further.

By eliminating these initiatives, the selection pool was reduced to fifteen initiatives.

Target service participants

Each of the remaining fifteen initiatives involved individuals or families at risk dealing with complex social problems addressed by multi-agency services. In the study sample it was desirable to have initiatives that cover a range of service participants. For this reason we sought to include initiatives that involve younger and older people, Maori, Pacific Islanders, and/or people with mental health issues. The programmes dealing with elder abuse (14, 18), Pacific families (17) and the DHB/Police initiative in Fielding around missing persons (19) all potentially met these criteria.

Apart from the iwi crime prevention plan which does not meet the criteria of being currently operational, no other specific Maori based programmes were identified by informants. It was important therefore that some of the case studies selected include components for Maori communities or families. For example, the Age Concern programme dealing with elder abuse (18) has areas of focus on Maori and Pacific Islanders. Moreover, individual Maori participants are taking part in some of the generic programmes, such as the Priority Offenders Programme (1) and the Integrated Service Response (20).

It also was desirable to select initiatives that allowed us to explore differences that may arise depending on whether information sharing is done with consent of the people to whom it refers or whether it is done without either their knowledge, and/or their consent. Each of these situations raises different issues regarding privacy protection and how agencies deal with information sharing arrangements. The Priority Offenders Programme (1) and the High Risk / High Profile forums provided a useful contrast in this respect. The information sharing arrangements in place for the Family Safety Teams (13) and Family Violence Response initiatives (11) could also potentially meet this selection criterion.

Information needs and support

Without exception the programmes dealing with 'wicked' problems at the social interface involved the sharing of information of a sensitive nature (e.g. personal health details)

about individuals or families between different agencies. This included programmes with both government and non-government organisations involved.

Moreover, some initiatives involved cross-agency technical infrastructure issues, such as database access, that needed to be resolved (e.g. Drug & Alcohol Services (9); Joint Employment Outcomes (3)). Several inter-agency initiatives, such as the Integrated Service Response (20), Family Safety Teams (13), High Risk/High Profile forums (5), Offenders Reintegration Project (2), and Family Violence Responses (11), provided examples of technical infrastructure arrangements that could highlight issues of interest.

Another case study selection criterion was to obtain initiatives with different partner arrangements and coordination models for cross-agency collaboration and information sharing, such as one government agency liaising with several other government agencies (e.g. EMBail (8)); several agencies meeting together and discussing the complex needs of participants on a case-by-case basis (e.g. Priority Offenders (1)); or the co-location of several government agencies and voluntary sector organisations serving individual participants (e.g. Integrated Service Response (20))

Regional spread

In order to obtain an understanding of information sharing practices throughout New Zealand, we wanted to have a regional spread of case studies as well as a mixture of rural, urban and metropolitan areas. It was acknowledged that programmes operating on a national basis (e.g. Age Concern elder abuse and neglect) were flexible and therefore could support this selection criterion.

Operational practice considerations

In order to obtain a wide variety of information sharing practices and experiences, we wanted to include case studies involving successful inter-agency information sharing arrangements as well as cases where information sharing had not been successful. In talking to agency representatives it became apparent that examples of different practice often can be found under the same programme, in different locations. We therefore selected six case studies under three programmes that met the variety of case study selection criteria and involved differences in information sharing practice and experience.

In total, eight case studies have been explored under the following programmes and initiatives (please see Appendix 1 for an assessment per case study area of how selection criteria have been met):

1. Multicultural Service Centre for Refugees, based in Wellington
2. Integrated Service Response: Linwood Service Centre
3. High Risk / High Profile forums: case studies in Hawke's Bay and Christchurch
4. Priority Offenders Initiative: case studies in Christchurch and Papakura
5. EMBail: case studies in Auckland and the Hutt Valley

We emphasise that there was no intention or attempt to evaluate the selected cases. Therefore this research makes no comment on issues relating to the efficacy or otherwise of the individual initiatives.

Empirical findings are described in the next chapter under the five programme headings within which the eight cases studied were located.

4. Case study research findings

Case Study Area 1: Multicultural Service Centre for Refugees

Programme	Short description
Multicultural Service Centre for Refugees in Wellington	▪ Service Centre for refugee communities in Wellington. ▪ Health and well-being action strategy. Actions are monitored by funding agencies. ▪ Involves over 20 government departments and agencies with multiple funding sources. ▪ Focused on meeting the multiple social needs of migrants including housing, income support, education, language skills development, psychological services, employment, health and welfare. ▪ Similar initiative operating on the West Coast for migrants and refugees. ▪ Involves NGOs, local government, central government and employers.

Background

Working under the umbrella of the Multicultural Service Centre for Refugees in Wellington, four different Wellington-based refugee service organisations were included in this case study. These organisations are part of the network of government and non-government agencies providing resettlement services for refugees who have entered New Zealand under the annual Refugee Quota Programme. Quota refugees are "*people whom the United Nations High Commissioner for Refugees has mandated as refugees overseas*" (Wellington Region Action Plan 2006, p.7). Selection for resettlement in New Zealand is based on those with the greatest need for refuge and protection. On arrival in New Zealand, refugees spend six weeks in the Mangere Resettlement Centre where they receive information on New Zealand society and are assessed for health needs and any other treatment required. From Mangere, they are relocated to different parts of New Zealand.

The agencies included in the case study are:

- ***Wellington Change Makers Refugee Forum*** – a refugee-based NGO representing twelve refugee communities in the Wellington region. The forum facilitates capacity building of refugee communities; represents the interests and concerns of refugee communities at the local and national level; advocates on resettlement issues; and provides information services to refugee communities throughout New Zealand. Change Makers is funded by grants, contracts for services, and in-kind support.
- ***ESOL (English as a Second Language) Assessment and Access Specialist Service*** – funded by the Tertiary Education Commission this service provides a range of assessments, advice and referrals to appropriate ESOL providers to migrant and refugee clients.
- ***Wellington Refugees as Survivors (RAS)*** – community based specialists providing mental health services to refugees under the Refugee Quota Programme. The agency depends on grants and donations.
- ***Refugee Services Aotearoa New Zealand*** – a not-for-profit, non-government organisation, registered under the Charities Act, 2005. The agency is jointly funded by

Each of the above organisations is funded separately. Some are funded by government organisations, and others depend on grants and donations. Collectively, the agencies included in this case study provide a range of resettlement services including assistance with housing, income and employment; language skills; mental health services; and advocacy and co-ordination services. Some service agencies are contracted on a regional basis especially for capacity building and training of people dealing with refugees. This can involve health professionals and social workers providing services as far a field as Masterton, Palmerston North, Napier and Nelson. Services relating to cultural competencies, including interpreters, are also provided in these areas.

The above-mentioned organisations also interacted with other agencies in providing services to refugees, including: Immigration NZ, Housing NZ, Regional/ local government, MPs, Ministry of Education – tertiary and primary, DHBs (Capital Coast and Hutt Valley), Police, Internal Affairs, Ethnic Affairs, Work & Income, CYF, Study Link, ACC, Mental Health Foundation, ESOL National Office, Courts (especially Family Court), Family Violence Units, and Corrections.

Information needs and requirements

- There is wide variation in the information needs of different agencies – from limited, abstract information needs to extremely detailed information needs. Moreover, information needs can involve different policy sector-related information sets.
- Implicit information needs and the lack of information sharing have an impact on personal safety and community safety. Schools in particular don't ask enough information from refugees or other refugee servicing organisations. This is risky as it means that front-line staff do not have information required to protect themselves.
- Sometimes the information requirements of government agencies clash with the cultural norms of refugees. For example, in some cultures if a young person (particularly a girl) is unmarried they are expected to live at home. For Housing NZ if there is overcrowding in a residence, adult children should live independently. Thus who does what with the information is as important as the information itself. Government department demands may lead to inadvertent social consequences that they do not anticipate, or understand.
- Newcomers often do not understand New Zealand values. Consequently, they do not know when information requirements can be compromised or changed (according to the different requirements of different agencies), or what is law and therefore will not be changed. Many new people think information requirements from different agencies are similar things.
- Information provided to newcomers on New Zealand is not balanced. It is either based on a marketing approach whereby everything about the country is fantastic, or it is focused on 'you must do XX or these will be the consequences'. People coming from countries with repressive regimes can be very frightened by the threat of consequences because they are unsure what this means in the New Zealand context.
- It is not enough to give clients information only once. People learn from experience; then the written information makes sense. Sometimes when people first arrive in New Zealand and in the Mangere Centre, they are too traumatized to take in the majority of what they are told.

Information sharing practices and procedures

- Personal information collected on individuals is shared between agencies in accordance with legal requirements. For instance, all clients sign a consent form to enable agencies to share information about their case. In asking for consent, consideration is given to an individual's privacy, but the paramount consideration is the safety of the individual, families, and the community. A formal complaints procedure is available.
- In some cases clients consent to information sharing between health and psychological service personnel.
- In some cases refugees give consent but are not clear what they are giving consent for. There are questions as to whether people understand what agencies do with their information and how agencies fit or collaborate together (i.e. who has access to the information for what purpose). Moreover, some of the consent processes are not comprehensive and limited in their effectiveness. For example, Resettlement may be authorised to work on the client's behalf, but the agency is not authorised to *release* information. In some situations this becomes unworkable.
- There are agency differences around what is valid information to share, or not share. There are also different processes around the collection, storage, retrieval and provision of information, and different expectations by officials from different agencies. When refugees are interacting with a range of agencies, these variations in information provision requirements can be confusing. For example, there are a wide range of rules with respect to the age at which you can do various activities in New Zealand (such as drink alcohol, drive a car, vote, live independently, or claim study assistance). How can people from different cultures and backgrounds be informed most effectively on these matters?
- There is a clash between government information sharing processes (top-down) and those of NGOs (grass roots). Government agencies tend to use an advisory / expert model in devising policy and then dictating this to NGOs.
- There are a lot of ad hoc networks set up to share information across the various agencies servicing refugees. This leads to duplication and information overload (e.g. five copies of the same information coming in via email). When staff get overloaded with information it is hard to sort out what is important.
- It is unclear what government agencies do with information they receive from NGOs. For example, reports are sent from ESOL to a government Service Centre electronically. The Service Centre is only interested in having received the report so it can mark a box for compliance requirements for ongoing funding. It is unclear, however, who sees the report, who uses it, or how it is being used by officials.

Information gaps and fragmentation

- From an agency perspective, there is a big gap in knowledge about refugees: what are their needs? What services do they require? How satisfied are they with the services they have received? Has resettlement been successful for them?
- The initial breakdown in information sharing is in how people are categorised and recorded at the point of entry into the country. Particularly with respect to people entering under the family reunification programme, there is more information that government agencies should know. A general solution would be to have forms designed to identify people's needs more effectively.
- The refugees who enter the service as quota refugees are easily identifiable, but there are a number of others who enter the country under the family reunification policy.

- A large number of organisations, government and non-government, hold bits of information on individual refugees, but no-one has the full picture. Common sets of information need to be collected to know what is actually happening around core areas, such as housing and health: what are people's needs? What is currently happening? What are the short and long-term impacts?
- Each independent body collates information independently. An effective reporting relationship is hard to establish. As a result, organisations fall back on forging personal links with individual central government personnel who are "*willing to talk*" in order to make them aware of services and provide information. This is personality dependent, ad hoc, impermanent and unstable. The longer the individual is in service, the greater the likelihood of good, sustainable networks developing.

Treatment of sensitive information

- Some privacy issues are delicate when staff members are dealing with people who may have had traumatic experiences in their originating country, but disclosure of that information is perceived critical for accessing and planning services. It is also seen as critical information with respect to the potential substantive impacts on the family and the community. For example, there may be serious health issues such as HIV, PTS or physical disabilities (such as amputation, artificial limbs or eyesight, hearing problems that affect the ability of the individual to access services).
- There are issues relating to the sharing of personal information across agencies. Often there is no place for establishing protocols to manage information sharing across agencies. Agencies gather a lot of information that other services could find useful, but they are not sure how to share it, or who to share it with. If staff members perceive a risk involved to staff or members of the community, they go to Refugee Services.
- Health agencies are different from other agencies in multi-agency arrangements in the sense that they are quite formal and have their own protocol for the protection of health information.
- There are a lot of different agencies involved in refugee's lives, and their personal information can be quite sensitive. There is sometimes an overlap of critical services, but no overlap of mandate regarding what information can be, or should be, shared. For example, ESOL may find that health, mental health, or trauma issues emerge in the classroom: do they need to do anything with this information? Who do they refer people to with severe depression? Sometimes if refugees receive the wrong information, or the wrong people are involved in service provision, it can lead to serious misunderstanding and result in a real mess.

ICT infrastructure, applications, skills and knowledge

- There is no use of 'shared workspace' functionality.
- Organisations rely on email distribution lists for information sharing.
- NGOs generally do not have ICT infrastructure support, technical skills or knowledge. These are not included in their core competencies. Moreover, there is no dedicated technological expertise available to NGOs because there is no funding for it.
- Across organisations involved people do not know what they do not know with technology. They are unaware of possible alternatives for technical support.

Barriers to effective information sharing perceived by research participants

- One of the major problems for refugees is cultural assumptions made about information by public officials. For example, assumptions that the use of language is consistent across cultures (especially through the use of acronyms); assumptions made about how people from different cultures or religions will think and what is important to them; and assumptions about what people know and do not know.
- There is a major information gap in the resettlement process in New Zealand. A comprehensive social-psychological assessment is carried out on each individual by the UN High Commission for Refugees prior to them arriving in New Zealand. This report may be available to the Refugee Services staff at the Mangere Centre (although this is unclear). Extracts are taken from the report for follow-up assessment in New Zealand, especially with respect to health and/or mental health. Appointments with specialists are made for the individual in the area where they are relocated. The local PHO deals with this. Critical information, however, is not sent to the Refugee Services agencies. In some cases, relevant information may be passed on to doctors or other medical personnel, but this information often has implications for other services, such as transport or disability care. In one case, a social worker finally did a home visit because an individual was not showing up to scheduled appointments to find this individual to be a double amputee: this information had not been shared with any of the relevant agencies.
- There is often no sharing of 'intelligence' within an agency and between agencies. For example, what are the needs, gaps and barriers to accessing language services in this country?
- Lack of, or breakdown in, communication between agencies focused on their own agenda causes hardship to clients. For example, Work & Income can cut off benefits or other forms of support (e.g. study support) because of single eligibility criteria (e.g. turning 19) without knowledge or understanding of the full picture or consideration of the social and family circumstances involved. This can create flow-on complications with other parts of the system, such as housing (rent) or employment. Similarly, CYF are taking children into care and placing them with families where there may be religious incompatibility, thereby placing the agenda of the organisation in conflict with the needs of the clients.
- When language difficulties complicate the ability of individuals or families to obtain relevant information, circumstances can become very difficult. Refugees are being asked to fit into boxes that do not work, because these boxes were designed for mainstream clients and government-centric purposes. Consequently, government departments are effectively creating problems instead of providing services that alleviate problems.
- Information issues arise when refugees do not understand the system, but also when people within the system (especially at the front-line) do not understand the system. For example, clients experience that 0800 operators often do not give out consistent information. In addition, they often say they cannot access a file (citing the PA) even for the purpose of making an appointment. Different things happen to different clients. For example, clients quite often can get a different response by simply putting the phone down and ringing again and getting a different operator. English speaking people, especially if they are sounding officially, are likely to be dealt with more efficiently. Similarly, dealing with front-line staff in person often depends on the skills of the individual operator at the time. This is frustrating for newcomers who are attempting to be independent and not use intermediaries. Documents usually are wordy and even interpreting some of the consent requirements are difficult. The personal circumstances of refugees is often complex and takes more than 30 minutes to work out, but a client has to wait longer to book in for a longer appointment time with Work & Income.

- Refugees experience different messages depending on the different people they speak to. For example, Community Law Centre, Refugees as Survivors, Local MPs, Refugee Resettlements may each have a different perspective. Refugees do not trust people to do the things they say they will do. Therefore, they tell their stories to multiple groups: 'the more people you tell, the greater the chance is that something will happen'.
- Further barriers to information sharing include the constant re-organising of government departments where there is a loss of continuity of personnel, loss of knowledge, lack of knowledge transfer and sometimes changes in processes and procedures requiring new compliance demands. As a result, NGOs face difficulties knowing whom to talk to, who is interested, and how to influence policy and funding decisions.

Enablers of information sharing perceived by research participants

- In this case study, information sharing between organisations could be assisted by:
  - Intermediaries being able to make appointments through Work & Income;
  - The sharing of information available from the Mangere Centre (e.g. information re health needs) with other agencies;
  - Using existing systems more efficiently. For example, front-line staff using interpretation services; and
  - Allowing clients to manage their own personal information and providing it to the people they want to – thus making privacy less of an issue.

Case Study Area 2: Linwood Service Centre

Programme	Short description
Integrated Service Response	▪ Integrated service centre for individuals and/or families with multiple service needs. ▪ Service Centre: Linwood – co-ordination of social services to individual clients with multiple problems requiring government services and interventions. ▪ Includes Work & Income, Career Services, Housing NZ, Health, Education, co-located in a single office (Christchurch)

Background

The Linwood Service Centre, Christchurch, is known locally as the Linwood Community Link and is the first of a number of integrated service centres operating throughout the country. The notion of integrated service response evolved as a result of the Ministry of Social Development (MSD) looking to re-organise the way services are delivered so that those people with more complicated problems can get the help they need. A service delivery model has been developed that focuses on 'life events'. Under this model three levels of service are posited:

> (i) Self help: whereby the client can identify their own need and find the information they need to meet their requirements by themselves. The Ministry is working on getting services online so that those people can service themselves quickly and efficiently at low cost.
> (ii) Minimal help: whereby clients require some additional information or assistance. Call centres are focused on providing this level of service.
> (iii) Major service requirements: whereby the client has multiple and/or complex needs and requires the assistance of skilled staff to meet their service requirements. Linwood Service Centre is designed to provide this type of assistance to clients.

In Linwood, the Service Centre is hosted by Work & Income who own the building where the Centre is sited. All of the office equipment in the Centre including computers, desks, furnishings and storage facilities, are owned by Work & Income. Other government and non-government organisations have been invited by Work & Income to make use of the premises to locate staff and service clients on an appointment, or on-site referral, basis. The office is fitted for wireless broadband so that other organisations can access internet-based capabilities. There are also two stand-alone computers that are not loaded with the MSD operating system available for other agencies to use.

Clients who come to the centre are primarily seeking income support or employment services. They undergo a 'client assessment' using a computer-based screening tool which identifies and prioritises their needs. Where appropriate, the assessment officer requests permission from the client to share their information with other providers, and refers them to either internal or external providers for case management. If the client has very complex problems and requires wrap-around services a case management meeting is arranged with all providers, or a referral is made to a relevant social worker.

Participation in this initiative poses some interesting challenges for agencies. The need for collaboration is accepted by agencies. NGOs are not set up or funded to do this work alone; there are other advantages to them to work in this way. For example, Work & Income pay for the building rental and provide the capital assets in the facility at no cost to NGOs. NGOs also receive referrals as a direct result of their involvement, and their funding is set according to the number of referrals they handle. On the other hand, not all organisations are set up in such a way that participation is possible. For example, IRD is not set up in a distributed fashion. They operate using Contact Centres and large service centres in order to use their resources most efficiently, therefore it is quite challenging for them to act in a collaborative way.

NGOs have been offered the Service Centre as private space to provide services from, but as yet this has not been taken up. Those agencies participating in the initiative have staff located at the centre on a part-time basis, as a satellite working space in addition to their central locations in other parts of the city.

Originally, Work & Income just issued an open invitation to share office space. The initiative has been operating for one year now and the partners are taking a more strategic approach towards providing services in an integrated way: collectively they are looking at what services are required and which services can be delivered at different times. A one-stop-shop is about the client accessing different information in the same place; this is about actively working with a person to improve their life circumstances.

At the moment the following organisations work out of Linwood: Work & Income, DBH, Housing NZ, Career Services, Workbridge, Tenants Protection, Single Women as Parents, Catholic Social Services, and the Salvation Army (Oasis Gambling Centre). Other agencies have been involved with the Centre, but no longer operate from there. These include: Inland Revenue, Community Probation, ACC, Kingdom Resources and Supergrans.

Information needs and requirements

- Over 250 people visit the centre each day. They are a mix of people, ranging from clients who are coming for pre-set appointments and are in crisis, to those who want support but have no appointment. Some are transfer-ins from other locations in New Zealand (or other parts of Christchurch) and some are new business.
- There are three assessors working for Work & Income who do the initial screening when people come in. The sole role of the assessor is to identify the client's needs, and the appropriate services required to meet those needs. The client group with complex circumstances is worked on intensively using a team-based approach.
- An electronic assessment tool is designed to ascertain what service is required; how urgent the service is; and who can best deliver to this particular client (i.e. what is the priority need). The tool asks high level questions to assess high level needs – e.g. housing, health, child care, employment, budgeting. Assessors can elicit additional information and this is sometimes included in the 'notes', but information outside of that required for assessment of income support eligibility is not routinely asked.
- The assessment process is client driven as they identify their own needs. It is a pathway to getting those needs met. The drawback of the tool is that you do not get what you need if you are not clear, or do not say clearly what you need. Some client's lives are so complicated that sorting out their needs is difficult.
- The assessment tool is drawing out more information from clients at an earlier stage than ever before. Complaints to MSD are down, and client satisfaction indicators are up 55 to 80 per cent. There is a 17 to 20 per cent increase in referrals from other sites.

- Staff perceive this relatively new assessment tool as 'work-in-progress': "*we are working out how to get the right balance between an individual's privacy and what staff need to know to provide the appropriate services. For example, how much do we need to know about health, gambling, addiction, probation, courts and justice, and how does this information impact on a person's income support eligibility?*"
- Sometimes the quality and quantity of information gained from clients depends on the attitude of staff. if they are seen to be non-judgmental they can obtain more information than is required for the assessment. The burden of judgment then falls on the individual staff member: "*what do I do with this information?"* The information may be confidential. Unless the staff member judges that they are personally in danger, another staff member is in danger, or the community is in danger, then the information may very well be ignored. Common sense is often applied – for example, ringing a person's GP on the spot, especially in a crisis situation.
- The partner's management group is working to develop a formal feedback mechanism that will produce useful outcome information. Current outcomes are too broadly defined. Stability in the client's life over a 3-month period is the key outcome indicator.

Information sharing practices and procedures

- If a referral is made to another agency, a 'client consent form' is filled out and signed by the client. The consent form has been designed by Legal Services in Head Office to conform to the Privacy Act. This is regarded as a critical tool as it lists all of the agencies requiring access to the same set of information.
- A copy of the paper-based client consent form is stored in a file at Linwood. However, other agencies have not asked for a copy so far.
- The assessment is printed and handed to the client. They then have the choice as to whether to pass that on to other agencies when they meet with them. Referral appointments are sorted out electronically. DOB/ Name/Address information is being shared with referral agencies.
- Referrals are made by hand-shake if relevant service workers are available on the premises and free at the time. Otherwise an email referral is sent by MSD staff, or a photocopy of the screening tool is left on their desk in the centre. The client identifies the other agencies they wish to have their information (e.g. drug & alcohol services, GP, probation officer): the referral form is given to the client in order for them to provide it to the relevant agency. The client also identifies the lead agency, or the lead contact person they want to work with them.
- The 'lead agency' is an important aspect of case management. Work & Income is the early identifier using the assessment tool. If a referral to another agency is made, that agency then takes over the information exchange with the client. They decide what is relevant information, or irrelevant information, and therefore what information goes back to Work & Income for income support assessment. The other agency is the gatekeeper of the information sharing at this point.
- Case managers work with clients through pre-set appointments after the initial screening process has been completed either at the Service Centre, or through a Contact Centre. They receive the assessment screen via email and use this to chat with clients about their individual circumstances. Sometimes, the face-to-face contact brings out things that were not picked up on the form, or a change in circumstances since the assessment was done. For example, a child may have subsequently left care or come into care, or a person may have a new partner. These things affect a person's income support entitlement.
- The Contact Centre has a screen similar to the assessment tool. This captures the person's circumstances and provides a pre-assessment of what services are required. They also set a client number for the case, and set up the appointments with the Case

- Service Centre staff receive regular training with regard to the Privacy Act and the Official Information Act.

Information gaps and fragmentation

- Staff are overcautious with using the Privacy Act in information sharing relationships between organisations. As a result, the Privacy Act slows down quality services targeted at clients with complex needs and with the right intentions.
- Sometimes staff get information that may negatively impact on a person's income support assessment. For example, a solo mother may come to a Strengthening Families meeting with a partner. This raises questions for staff members: in what circumstances can this information be shared, and with whom? How can it be shared – informally or formally? In general, as a result of the Privacy Act, staff perceive that they cannot share personal information with other organisations.
- Agencies have different agendas and therefore use information in different ways. This sometimes leads to information sharing 'conflicts of interest' between frontline staff of different agencies. As a result, information sharing doesn't happen or need to be negotiated.
- Problems arise through procedures not matching the requirements of particular individual's situations. For example, when people come out of prison, they do not have the multiple identification requirements necessary to get some income support assistance. That is, they require photo ID, their birth certificate and two forms of validated ID (i.e. showing they are living at a particular address such as a power or phone bill). These requirements are aimed at the small percentage of clients who have defrauded the agency, but these strict business rules prevents providing services to clients in need.
- Feedback often occurs directly between professionals, but is not yet formally captured.
- Monitoring of the service is done on an EXCEL spreadsheet. It is up to the case managers to fill in the information – if they remember. Only informal information is available from the NGOs, as the spreadsheet is completed by MSD staff only.
- There is no centralised database that all partner organisations can access. At the moment the screening summary sheet is (i) emailed; (ii) photocopied; or (iii) handed to the client to pass on to the relevant service.
- The Contact Centre in Christchurch (but not in Linwood) needs to be able to direct clients to services. They have to have a national basis for their information therefore manual processes are not feasible. The 0800 number may be answered in Auckland.
- The long-term plan is to open access to all information. The Linwood Service Centre as an island is not a sustainable solution.
- Staff perceive the need to resolve information sharing problems in a practical fashion. A balance is necessary – not letting information sharing get too much of problem so that it inhibits success, or creates a bigger problem than is necessary.

Treatment of sensitive information

- The partner agencies work together to work out how to manage privacy issues. It is about sharing information, not using it in a punitive way. The sharing of information is used to build trust between the case worker (Work & Income), NGOs and the client. It is an ongoing process to identify clear lines around what information is used for what purposes.

- The Privacy Act is used to minimise discretionary mistakes. Staff err on the side of caution. It is a public management challenge to work within the rules and protect individual privacy with so many cases involved.
- Privacy can be an issue for clients, but only for those who do not want to be in the game: if you do not want help, you do not get help.
- It is made clear to the client that information about personal circumstances will not be "*dobbed in*" to Work & Income or other agencies, but at the same time an agency does not support bad or unlawful behaviour.
- Staff have concerns about the protection of an individual's privacy caused by the open office plan design: for instance, clients potentially could listen into conversations between staff and other clients; clients potentially could look at personal details displayed at computer screens from a distance.
- NGOs are not so rigorous about the safety of information required by government agencies. They do not understand the constraints.
- Some NGOs have privacy officers who monitor compliance; other NGOs do not have the resources for privacy officers.

ICT infrastructure, applications, skills and knowledge

- Linwood operates on a web-based system sitting on a server on the premises. Because it is web-based it has inherent security problems. However, the information cannot be transferred outside the MSD system. So, at this point the screening tool is only available to MSD staff. An inter-agency facilitator is currently emailing each agency the referral appointments. The calendar functionality in Microsoft Outlook is used but other agencies can not access it remotely.
- Five providers want to trial the screening process for those clients who come directly to them. There are issues of technical interoperability between the systems of the partner organisations. It is a stand-alone web-based system.
- The office is fitted for wireless, and there are two stand alone PCs that do not have the MSD operating system on them so they can be used by other agencies. Housing NZ staff bring their own computer and hook it into the MSD server. DBH has a portable office. The Community Probation officer has a laptop. All of the other organisations work manually, especially NGOs who do not have the resources for portable equipment.
- The flow-on effects of the assessment tool are not yet sophisticated. For example, lead agency and information security depend on co-operation between professionals using manual processes.
- There is technology that allows for collaboration that is not used by the Centre. For example, there are capabilities to send tasks via email and once the task is completed the client case is updated automatically and so are the client profiles. This is not yet being used to capacity. Authorities and access between agencies has to be resolved.
- Technology solutions are not always the answer. For example, electronic calendars can help, but sometimes a crude spreadsheet works just as well. Outlook is likely to be used across agencies to resolve the interoperability issue.

Barriers to effective information sharing perceived by research participants

- "*Legislation (e.g. the Privacy Act) has been introduced for worst case scenarios. In 99 per cent of the cases staff are fine. However, if they break the law they do it for the right reasons. Common sense needs to prevail*".
- Issues around privacy protection are not emerging in the needs assessment with the client, but in relationships between organisations.
- There are Privacy Act issues around sharing medical information between agencies.

- The client controls the information provided to the various partner organisations. For example, the client needs to pass on the referral form to the agency concerned. Moreover, service provision to clients could improve by finding a way to avoid specific consent for each individual case.
- NGOs face an awkward situation in the current environment of fiscal prudence. They need to attract funding by proving the value of participating in an initiative of this order, but do not have the information resources or technical capability to do so.

Enablers of information sharing perceived by research participants

- There is a hard balancing act between common sense and getting the job done. The relationships around town you have and the trust you earn are critical for information sharing and doing your job effectively. Community knowledge and word-of-mouth are strong in a place like Christchurch. It would be beneficial if organisations would have an information sharing protocol between each other.
- At the moment, there is only a service assessment done for Work & Income. Staff would like to see service assessments done for all partner organisations.
- Linwood managers would like to see a shared workspace developed and they have developed their own concept design (refer: Model office concept @MSD). This would include a collaborative booking system. It would enable joint responses and the ability for more than one agency to share the lead in case management. There is a question of funding, and of IT understanding on the part of the service providers.
- It would be ideal to have the client present at the personal hand-over between the service assessor and case manager.

Case Study Area 3: High Risk/ High Profile Forums

Programme	Short description
High Risk / High Profile Forums	▪ Monthly meetings held for planning the management of high risk offenders once they are back in the community. Involves the agreement of release conditions. ▪ Does not involve the prisoners themselves (i.e. agency planning purpose). Planning can start up to eight months prior to release, but more often focused on those four and two months prior to release. ▪ Involves Corrections (prisons' management, probation, and psychological services), Police and community service providers ▪ Type of information shared can involve offender history, personal details and service needs. ▪ Eight forums that cover the whole of NZ. ▪ Uses a national database because of the mobility of the prison population.

Background

HR/HP forums are an internal Corrections Department initiative seeking to improve release arrangements for prisoners who are categorised as high risk and/or high profile based on their offending history; behaviour within the prison; likelihood of re-offending and/or risk to the community; and the level of public interest in their release. The recent Corrections Amendment Act, 2009 provides for an increase in the amount of information sharing on highest risk offenders about to be released from prison. The previous Act (2004) only provided for the sharing of information *following* release.

The intention of the HR/HP forums is to improve the interfaces between the range of agencies involved in the release and the management of prisoners in the community. This includes improving communication and co-operation between the various arms of the Corrections Department (Prisons management, probation, and psychological services). It also involves improving the relationship between the Department and Police and other government and non-government agencies involved in managing prisoners once they move back into the community.

Prisoners are identified as high risk (HR) based on a number of identifying flags within the various Corrections databases including psychological and behavioural risk assessments, breaches of prison discipline, length of sentence for violent offending, and child sex offender classifications. These ratings are recorded electronically, and once they are invoked they automatically create a record in the HR/HP database. The HP classification is an in-house classification that includes "*any prisoners who are likely to attract media attention or arouse public reaction beyond that which might be reasonably expected*" (Corrections Circular, 25 August 2008). Prisoners meeting this criterion but who are not classified as HR are added manually to the database at the discretion of the Corrections staff.

Access to the HR/HP database is on an approvals basis and separate authentication is required to log in. While the data in the database is sourced from the central Corrections

operating system 'Integrated Offender Manager System' (IOMS), it is a separate system and does not update any information in IOMS.

This initiative involves managers from a range of prison services (including corporate, health, sentence planning and reintegration planning), and those of other branches of Corrections – community probation and psychological services. In some cases, Crime Prevention Officers from within the prison are involved. The HR/HP forums are attended by senior personnel (e.g. Prison managers, Principal Psychologists, Probation managers) from within Corrections. NZ Police intelligence staff or CIB officers also attend in some areas. Under the forum guidelines CYF can be invited to meetings to discuss particular cases if necessary. This doesn't actually happen in either region studied but follow-on meetings do take place between members of the reintegration team and other agencies. The chair of the HR/HP forum is rotated between the three branches of correctional services: community probation, psychological services and prisons.

Prisoners are identified eight months before release, and the forum participants populate the database with release arrangements as they become available. The HR/HP database contains fields for Name / Dates (entry into prison; release date) / Offences / Previous offending / Length of sentence / Intended release date / Information from each service, including Police / planning progress. Concerns or issues that need to be addressed before prisoners are released in order to minimise the risk to the community are identified. Attendees take responsibility for ensuring that, in their area of responsibility, appropriate arrangements are made to address these issues.

There is another internal liaison meeting focusing on the management of complex cases that involves Corrections, social workers and custodial managers. It deals with complex cases where people are identified as problematic. They pose a high departmental risk, rather than necessarily a community risk. There is common ground about custodial and management plans for these people, and it often involves a lot of health information. Representatives from this group are starting to attend HR/HP.

Case study respondents described the HR/HP initiative as a bridge between sentence management and release management. They indicated that as a result of the forum they have more confidence that HR offenders are both treated effectively *in* prison, and that the management of that person once they are released back into the community is as good as it can be and that the necessary support is in place. Respondents see this as a positive move towards a more integrated '*offender planning'* process, and an effective means of reducing risk to the community.

Information needs and requirements

- The common thread is '*what do people need to know?*' It may only be the prisoner's intended address, and what their likelihood of re-offending is. Community safety is the paramount consideration. The key information that managers are interested in is where the person will reside in the community. Other planning hinges on this information.
- The focus of the forum meeting is on the profile of the prisoner and their offending patterns. What are their reintegration needs – residence / relationship issues / victim issues / rehabilitation needs / programmes to reduce the risk to the community? Forum members are looking for information on completed programmes, intelligence from crime prevention officers (working as intelligence gatherers within prisons), and any reports on their behaviour while in prison.
- The database provides input to the preparation of pre-release planning. The primary focus is to identify reintegration and rehabilitation needs so these can be addressed on

- An eight-month time period for preparation before Parole Board is adequate because of the number of people who have to intervene before release. A longer warning time is useful, because it allows time to make things happen for those with more complex needs. The release process is smoother.
- Managers second-guess what information the Parole Board requires. Before HR/HP it was very much a mechanical, tick-box approach. The HR/HP forum is more about informed decision-making and planning to address release needs.
- Parole Board's will now take 'unproven' information into account, but only things that are proven or substantiated are going into the formal reports. Staff are conscious that the reports are discoverable.
- For Police CIB, information provided at HR/HP forum meetings is 'in process' and not finalised. It therefore is of little value for investigation purposes. Information may be passed on to the Police Intelligence branch if it is relevant, either informally or via email.
- All custodial staff keep extensive daily records of prisoners – at entrance to the facility; risk assessment done on every new entrant into a Unit (B14); any custodial incidences; any changes in circumstances – health/ family/relationship. The primary source of information is prisoners/ staff conversations, but formal reports (e.g. B14 or incident reports) are entered into IOMS. Evidence / file notes can work to protect staff. Sentence Planning reviews – file notes are recorded on all interactions with prisoners. Hard copies of the files travel with prisoners when they are transferred – warrants/ telephones/ B14/ segregation records/ sentencing notes/ Police summary of facts.
- Reintegration Case Workers (RCW) are assigned to help prisoners coming to the end of their sentence to establish a reintegration plan including accommodation, employment, psychological care, community support, and health care. If a prisoner is referred from the HR/HP system the number one priority is to establish accommodation intentions and get a verified address on release.

Information sharing practices and procedures

- Principle 11 of the Privacy Act gives a mandate to operate and staff are hardly restricted. A common sense of '*safety first*' over-rides privacy concerns: *"The bottom line is that I would rather be hauled in front of the Privacy Commissioner, than in front of the Coroner's Office".*
- Privacy is restricted to health issues and it is usually not relevant to re-offending therefore doesn't need to be on the table anyway. Only information that is relevant to the task to be achieved is shared; not all of the information known about a person.
- Information is provided by chaplains, health workers and programme staff. As professionals they know how to share vital information without sharing actual, factual details that might breach a person's privacy.
- "*Conversations between professionals at the table are not always suitable for expressing in formal documents exactly as they are said*".
- There are debates about the appropriateness of information sharing. For example, psychological services debate whether information they hold should be shared with Police personnel at the table. The critical question is whether the information they hold poses a risk to members of the community, victims, or to the prisoner themselves.
- Everyone is concerned about using information appropriately.
- Generally, the things discussed in the forum are in the public domain. Other things may be discussed, but are not included in the formal notes. Staff are conscious that a person may be endangered if they are cited as a source of information, and the file is accessed by an inmate through their lawyer. The balance between 'soft' and 'hard' information shared in the forum is about 2:98%.

- Professionals who are at the forum meeting all have a community safety agenda. The disclosure of information is for a specific purpose – discharging duties as Public Servants. The information shared is relevant, useful, and focused on operational efficiency. It is about sharing the stress and responsibility for managing the release into the community of a difficult group of people.
- Information sharing is a two-way thing. It is about safety and common sense – "*doing the right things, rather than doing things right*". People need to know stuff to do the job properly.
- At the meeting Police can share information on the release address, threats made by prisoners (or against prisoners), and gain information about issues that might be relevant to the public or about release conditions that the Police may be required to manage. Police involvement is invaluable to Corrections staff because they are able to provide information re family and victims that need to be taken into account in release planning. For example, prisons do not know if a Protection Order is in place. Corrections is never given much information about actual offending (apart from the category of offence convicted on) and therefore it is difficult to plan release safely.
- There is an HR/HP firewall. It is assumed that if you are at the table then you are privy to specific information sets. This includes Police personnel. The role of the Police has evolved. At one stage Corrections instructions prevented sharing HP information with Police. Now all HR/HP names are made available to Police representatives on the forum two weeks prior to the meeting so a cross reference with Police databases can be made. Prior to the HR/HP forums being established Corrections staff were entirely dependent on the knowledge of management staff one-month in from release. Police are more graphic in their data presentation. They have sentencing and social data which is otherwise unknown to the Corrections staff.
- With the exception of Police, all other forum participants are Corrections staff, therefore it is essentially an 'in-house conversation'. The prison reintegration teams work with CYF and Work & Income separately to the forum. Information is shared based on established relationships.
- Information sharing protocols were released by Head Office in 2008. These have been helpful in setting out how the forums should be run – how it is chaired, and who is involved. They operate with a shared chair, so people take equal responsibility for the success of the meeting.
- The HR/HP forum meetings have led to a situation in which information sharing can happen more freely now that staff know the other people around the table. Moreover, the forum provides more context to shared information; it is not a 'tick box'.
- The lines of communication have been significantly improved and have overcome the silo operational management that was taking place. There are information sharing and feedback loops. The quality of the information is better because there is an assurance that action will be taken.
- The intention of the HR/HP initiative is to proactively manage risk. The process may be handling people unnecessarily, but the effort is worth the risk.
- People come to the meeting very well prepared. This is the key to making the meetings move. Follow-up tasks are allocated at the meeting, usually for additional information gathering. People take responsibility for this, and are held accountable for it by the group at the next meeting. If there are any changes required to the database following the meeting these are usually organised by email or telephone.
- Some managers take their staff into the HR/HP forum meetings, as they have relevant information.
- The forum has other spin-offs in terms of relationships. Other forms of informal information and intelligence are shared now that people in the different professional groups know each other. Over the duration of the forum operating managers are more confident that the information they are sharing (including that of a sensitive nature) will be treated appropriately. There has been a build-up of professional trust.

- HR/HP information is only available to the members of the HR/HP forum, but only a limited number of people can access or change the information on the system (i.e. nominated administrators). Only administration staff (and possibly the forum chair) can print from the database. Administrators also provide information on the results of Parole Board hearings, and record and distribute notes from the monthly HR/HP meetings.
- The use of the IOMS system has broken down personal information sharing. The most common form of information now is electronic. Computer records can be used as evidence though so you have to be careful what is written and how it is written. It tends to be very 'PC'. Staff have to be concerned about the accuracy and professionalism of the material kept on the database. All staff are mindful of other disciplines around case notes. Everything recorded is evidence based, brief, and OIA compliant. Staff are conscious of the fact that the recorded information needs to be able to stand up in the case of an enquiry.
- The database doesn't restrict information sharing with each other. This can be done by direct communication. The right kinds of information are at the table. What isn't on the computer is provided by people present from their own sets of knowledge.
- A fairly free flow of information is available on IOMS between staff employed by Corrections. There are flags within the system that notify PCOs (front-line staff) that this person is part of the HR/HP process. There are flags that indicate there is a transferability restraint. It is a method of sharing with the custodial staff that this person is of interest to the management staff. They then pay extra attention and can raise any concerns they have with the relevant manager/s.
- There are two to three releases per week. Custodial staff find out who the Probation Officer will be and speak to them personally at least one month prior to release. A 'heads up' is provided to other professional staff informally. It is about the quality of information. It is a professional courtesy to provide as much information as possible. Good information sets are based on stable, long-term relationships. You need to know things to do the job. It is about community safety, victim protection and victim minimization.
- In smaller towns, Parole Board members track down the Custodial Officers and ask for information. In the early days Sentence Planners and Parole Board members were co-trained.
- Sometimes two managers from the same service attend the same meeting just to cope with the volume of prisoners discussed in these meetings and to make sure that nothing is missed. There is no time to deliberate case management style. "*If it is not relevant; it is not shared*".
- Information sharing is difficult for new staff, but easier for more experienced staff who know personnel and have built up trust relationships. Information sharing without prisoner's permission is OK between prison staff, probation and psych services because it is collegial information sharing on a needs basis.
- Crime prevention information is based on intelligence gathering, not on evidence therefore it can be suspected by other staff. If accepted, it can be invaluable.
- Any release of information from forum (to other staff) has to go through the Chair.
- Sentence planning officers create the Parole Board reports. They check that every piece of information from all parties is available to the Board. These reports are the link to make sure that good quality information is provided to the Parole Boards.
- There is regional variation re input of Police. In Christchurch, Police check the suitability of release addresses in all cases. In Hawke's Bay this is not routinely done unless someone on the HR/HP forum specifically requests it. Furthermore, in Hawke's Bay, the Police do not use the HR/HP database because they do not see value in the information contained in it [NB: In Christchurch, Police Intelligence officer attends HR/HP; in Hawke's Bay a CIB officer has the role]. If the Police representative in Hawke's Bay has any concerns about a prisoner to be released it is brought up at the meeting, especially if Police wish their concerns to be made known to a Parole Board.

- Reintegration Case Workers (RCW) engage with prisoners to get planned accommodation information. Prisoners give permission/ consent (by means of a signed form) for this information to be passed on to Community Probation. RCW contacts pre-assigned
  Probation Officer to get accommodation checked out. If the address is not approved by Community Probation, the RCW explores alternative options with the prisoner. Where supported accommodation with the Salvation Army is used, the prisoner gives permission for information on their criminal record and any associated risks they pose to be passed on. Prisoners sign information release forms if they are willing for RCW to share information with service providers on their behalf.
- Psychological Services in particular didn't think they could share information with other parts of the service, or Police. Head Office guidelines clarified the situation.
- Members of the HR/HP forum act as a conduit for information to Unit Staff managing the prisoners directly, and service staff from the other agencies. For example, Sentence Planning representatives pass on to custodial staff what information is required (e.g. planned address on release). Custodial staff obtain the information from inmates and pass it back to the Sentence Planning staff who arrange for the HR/HP database to be updated.

Information gaps and fragmentation

- Detailed health information is not shared, but critical information is required to do a professional job. If information is critical it is possible to request a Psychological Service report release, but this is rare as the information is available in other forms from other services (e.g. the Parole Board report).
- Not all of the front-line officers know about the forum, and only limited information from the forum is shared outside it – if management staff have any concerns, or if there is release information they require.
- Some regional staff point at a lack of communication and information sharing with H/O, which creates uncertainty.
- Although IOMS is the general operating system, it contains a number of discrete databases with restricted access. Custodial officers in prisons, Probation Officers and Psychological Services each have their own separate databases. Each part of Corrections has their own 'business rules'. Information on the HR/HP database is entirely separate from normal, clinical file management processes. HR/HP members collate information from the separate databases of IOMS that they work from and they are imported to the HR/HP database. This is either done by authorised personnel, or sent to the prison administrators who enter it.
- Risk ratings used for populating the IOMS system are not necessarily the best. For example, people with Offender Warning Ratings (OWR) ratings do not necessarily pose a risk to the community. They are more relevant to Community Planning and Probation Services' (CPPS) operations. The Child Sex Register (CSR) threshold may also be too high. It was set at a national level without consultation with local staff and does not meet operational needs.
- Different agencies have different pieces of information for different purposes. For example, not all victims register on the Victim Notification Register (VNR) – i.e. that they wish to be told when the offender is released from prison. However, if there is a VNR flag on the prisoner's file the RWC will contact Probation who checks if the planned release address is within distance of the victim's address. Corrections are not told who the victim is for anonymity purposes.
- If an inmate has a flag against him on the Victim Notification Register, but no other risk flags he will not appear on the HR/HP register. In this case, the victim information is sometimes not known to the managers and inappropriate placements on release can be made.

- Assessments could be done prior to release in order to inform Parole Board, but there are Privacy legislation considerations here. It would only be relevant if they pose a risk to the community.
- PCOs are not picking up and acting on issues that arise at Parole Board meetings quickly enough. They are leaving it until the next hearing is looming and for some things this is too late.
- Some prisoner's sentences are short and therefore they do not have a Parole Board hearing and do not go through this pre-release planning but they can still be a risk to the community.
- Police are only given information from Parole Board Hearings if they have made a submission. [NB: this varies between regions – in Hawkes Bay, by request, the Secretary of the Parole Board calls the HR/HP Police personnel directly following hearings to inform him about necessary actions, or release arrangements]. The usual process is that the action and information flow moves from the Parole Board to the Probation service to the Police (following release).
- Corrections struggle to get information required by the Parole Board. The mind set of the Sentence Planning staff has to be changed about how they engage with prisoners and what information is required to provide good quality information to the Parole Board. Information is not complete at the eight-month point, but should be more complete at the one-month point.
- Prison officers can be compromised because they are not provided with all the pieces of information regarding the person they have care of. For example, a prisoner may ask to go and stay with X on his release. If the RCW rings X to check this arrangement he is breaching the law if a Protection Order is in place. Prisons are not notified when Protection Orders are made.
- It is unclear to front-line administrative staff how much they can tell [often distraught] family members. There needs to be a balance with privacy procedures whereby the rights and needs of the family are considered as well as those of the individual.
- Professionals are sometimes being exposed to danger without their knowledge. For example, if an inmate has a history of assault on female officers, he may be a risk to the female staff in the accommodation facility he has been accepted in, but that information is not been passed on to the service provider.
- There is an ongoing duplication of risk profiles between the different organisations involved in HR / HP. For example, treatment relationship versus custodial versus intelligence. Collectively, staff are trying to achieve management oversight for those released who are of concern. Possibly, one risk assessment system could be developed. It is complicated by the fact that Police and Corrections also use different classifications for HR offenders.
- Information between the Immigration Service and Corrections is limited. For example, Corrections have no way of picking up on Deportation Orders and therefore may release people back into the community when they should be leaving the country.

Treatment of sensitive information

- In general, staff know when what is being said is not in keeping with the Privacy Act, but sometimes it is necessary to make people aware of particular information because of safety issues.
- Custodial staff do not need better access to medical information. If the staff know prisoners well enough they will very likely know what's going on. If staff read the written records as well, there is enough information available to do the job.
- Health reports belong to the inmate. Psychological Service reports are the property of Corrections. They have a confidentiality rider: therefore, information can not be shared with providers, but information is shared informally for risk assessment reports. For example, Psychological Services recommendations go to the Parole Board and the

- In the case of a health diagnosis where the prisoner is eligible for a needs assessment, information on the prisoner has to travel with the inmate and be provided to providers. If an inmate is in the care of the Forensic Team they have to obtain the permission of the prisoner to their health information and criminal record to be made available to providers. There are networks of community providers and formal sets of information that are provided to them. Different providers have different requirements regarding what they need to assess suitability of the client for acceptance into the service.
- Medical staff often tell Prison Officers things to clarify whether the person they are dealing with is a suicide risk, or has anxiety, or depression. All of these things affect their care. But it is always necessary to be compliant with a community mental health service.
- Prisoners sign a 'release of information' in some instances which provides leeway for prison staff to share some information across services. Health notes cannot be passed on, but health-related information can be verified.
- Health staff can put relevant information where necessary on a template report such as a SMP 35 – Advice to Sentence Planners. For example, 'methadone programme' or 'surgery'. It is a case of staff knowing how to interpret the information they get from prisoners and other staff members. There is also 'Advice to Unit Managers' forms where change in health status is notified. These do not provide medical details but provide information on signs to look for, and act as guidance to custodial services.
- Salvation Army has their own consent forms that give broad access to all kinds of personal information including physical and mental health.
- In Christchurch, all hardcopies of the database distributed to HR/HP members are numbered and counted back in following the meeting and then are shredded by administrators. In Hawke's Bay all HR/HP members keep paper-records of the database. "*This will only last until it goes wrong*".

ICT infrastructure, applications, skills and knowledge

- The HR/HP database is an Access database in IOMS. The information in it is incredibly brief and only provides a notated-form of the details needed for release planning. Different sources of information are relied on by managers to collate a picture – sentencing plan; parole report; incident reports and so forth. If more information is required, custodial officers are asked to provide this directly.
- The HR/HP database is fairly clunky and not user-friendly. There is room for improvement there. It has been designed to suit IT purposes rather than for the end-user. For example, the search function has been changed and it is now less useful.
- IOMS includes the warrants from the Court. This is entered by the Receiving Officers. There are three checks done to ensure its accuracy. There is some limited access to Police information. For example, links to aliases and previous offending.
- The HR/HP database is only accessible to Corrections staff; Police do not have direct access to the database. Police are sent, via email, a spreadsheet of the HR/HP programme with names and relevant information on it (e.g. prison facility/ prison dates/ Board hearing date/ Alerts and classifications (e.g. child sex offender) and any victim notification requirements. Police then check against their own database and manually copy and paste relevant information from the Police database (NIA – National Intelligence Analysis) to the XL spreadsheet. This is then emailed back to the prison administrator to be manually transcribed back to the HR/HP database. Police have to trust that the data is accurately recorded.
- External email and internet access is very restricted in Corrections to authorised users only. Custodial staff are careful about the contents of emails. They file notes and incident reports and these are kept as formal information.

Barriers to effective information sharing perceived by research participants

- Barriers are related more to communication breakdowns, behaviour and attitude of the professional groups to each other than they are legal. All staff are bound by the Privacy Act. Medical staff are also cognisant of the Mental Health Act, and custodial staff of the Corrections Act.
- Generally, there is a strong perception that safety overrules potential concerns around privacy. However: "*the Privacy Act gets pulled out as a reason for not doing something*".
- Barriers are related to uncertainty about whether important safety-related information can be shared with other service providing agencies. There is a lack of education in areas of risk. The default position of staff in these situations is not to share information. For example, in relationships between Corrections and Work & Income: "*legalities come up. What does Work & Income need to know? We have to be allowed to give them as much information about potential [safety] risks. People are hiding behind the Privacy Act. There is a risk for Work & Income of making big mistakes as a result of not having enough information*."
- Barriers are related to a lack of information about legal provisions. Are the right people getting the right information? 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. Another example is that where prisoners need to be hospitalized it is expensive and time-consuming to put in place a plan of care and arrange appropriate security. But hospitals won't release information to custodial staff about the health issue so that appropriate planning can take place (e.g. will they be in overnight, or for several days; will they be mobile or incapacitated; will they need particular equipment?). Yet, the hospital staff require co-operation and information from custodial staff so they can do their job. How do we keep each other safe in these circumstances?
- There are challenges to get the correct people at the table every month.
- There are questions whether all categories in the database should be there.
- Case volumes (in Christchurch) are unmanageable. Already some criteria for the forum meeting have been changed (e.g. originally included all young persons, and all sex offenders) as they were too broad. They have been narrowed down to make them more manageable. Police disagreed with some of the withdrawn criteria, but were no party to the decision as an external party.
- Awareness that some information held by Corrections staff could be of use to other agencies, but there is no mandate to pass it on. For example, why cannot relevant information be passed on to Work & Income so that they could make an appropriate work placement? Corrections are aware of some system rip-offs (e.g. income support), but have no ability to let other agencies know.
- There is variation between service providers (e.g. CYF/ Corrections) due to different regimes (e.g. protocols) and understanding of information sharing protocols. Different interpretations of the Privacy law and information sharing possibilities leads to further variation in service provision.
- There are grey areas wrt information sharing with community-based service providers. For example, government agencies often have formal protocols set down in writing (e.g. between Corrections and CYF), but many other agencies assist with practical needs on release. It is unclear how much can be shared with them, and how the Privacy Act can be interpreted around that. A consent form from prisoners often overcomes these problems.
- Personality problems and parochialism between the branches of the department create barriers to information sharing. This is reinforced by different groups having access to different information sets. *"Integration should be real, not hypothetical"*.
- Volumes of personnel looked at during the meeting impacts on the quality and quantity of information sharing. Quality is also influenced by the way the information is

- Emphasis is on the release and the reintegration of the offender; not on the safety of the victims.
- What is relevant information can be very different to Police and Corrections. For example, in the case of direct release (i.e. prisoner's have completed their sentence and do not need to appear before a Parole Board) there is no intelligence information on their release plans.
- Credibility of the database with respect to accuracy and reliability is an issue.
- There is no common training or understanding of the Privacy Act for operational staff.
- Strict data controls exist within silos of the department, and these are not necessarily compatible.
- There is a more open collegial interface between certain levels of managers as a result of HR/HP but not necessarily between operational staff and this can be problematic.
- Trust issues exist between staff from Corrections and Police, and even within the different branches of the correctional service. Patch protection occurs.
- Information can be misused but this is difficult to manage. For example, debt collectors can publish prison officer's name and addresses. This leads to a 'dumbing down' of information you are willing to make available. Head Office monitors this to try to control it.

Enablers of information sharing perceived by research participants

- All members of the HR/HP forum have the same goal – ensuring community safety. There are ways of sharing even sensitive information in such a way that the community can be protected without violating a person's privacy. It comes down to a trust in each other's professional opinion based on information that they may have that is not able to be disclosed. It is person specific, and a case of professional ethical standards. Sometimes people have to accept the reliability of information based on good faith, relationships, and professional respect. It is a reciprocal process.
- Relationships building within and between agencies is crucial. Therefore, regular face-to-face meetings are very important. However, there are budgetary constraints on having these meetings (e.g. travel).
- If the forum were expanded (e.g. to include community-based service providers, or other government organisations) the conversation would be more reserved.
- Greater disclosure of medical information would take the guess-work out of the custodial officer's job. Access to substantive information could modify the treatment or care. You cannot assess the full extent of the risk you are dealing with if you do not have the full information set.
- There needs to be an interface with the National Intelligence Database (NIA) of Police. Usefully release address, release dates and physical attributes could be cross-referenced.
- Forensics would be valuable to have at the table.

Case Study Area 4: Priority Offenders Initiative

Programme	Short description
Priority offenders initiative	▪ Providing wrap-around services for prolific offenders. ▪ Voluntary participation on part of clients. ▪ Involves 7 agencies who meet together and discuss the needs of participants on a case-by-case basis: Police, Probation and Prison Reintegration Officers, Housing NZ, Education, CYF, MoH, Work & Income. ▪ Information sharing protocol developed in conjunction with the Office of the Privacy Commissioner. ▪ Types of information include criminal histories, personal details and service needs. ▪ Pilots running in Kaikohe, Papakura, Rotorua, Flaxmere, Porirua, Christchurch.

Background

The Priority Offenders Initiative (POI) is a crime reduction initiative, targeted at a small group of offenders who are attributed with committing a disproportionate amount of crime in their local area. The individual is initially identified by the NZ Police based on their offending history. Senior managers from a range of government departments check their departmental records to identify and prioritise needs in the individual's circumstances. He/she is then visited by a member of the NZ Police and the senior manager of the agency regarded as being best placed to assist the individual to stop, or reduce, their offending.

The initiative arose from analysis of 'crime families'. For example, an empirical analysis was carried out in by Police in Christchurch. It was identified that two per cent of the apprehended offenders carried out over 20 per cent of the crime committed in the area. The same family names repeatedly appeared. Ten families were identified in the Christchurch area as being a focus for intervention. The purpose of the initiative is to provide a high offence rate individual with the support and assistance in addressing the social, cultural and economic pressures in their lives and thereby provide them with an opportunity to change their offending lifestyle.

The identified individuals are invited to participate in the initiative and do so voluntarily, usually in consultation with their family/whanau. Offenders do not receive any services that any other client would not receive, but they are given priority of service and entrance barriers are lowered. The senior managers who work directly with the client have the ability to assist with unblocking access to services. Management and case worker discretion is involved.

There are a number of agencies involved in this initiative, and the composition of those agencies may alter depending on each geographical area where it is implemented. In general, key agencies include NZ Police, Work & Income, Community Probation, CYF, NZ Housing, and the Ministry of Education. In some areas, the DHB or local health service providers are also involved. Although a number of agencies work together, Police commitment, ownership and resources drive the process at the local level.

Governance and managerial arrangements differ in the geographical areas where the initiative is implemented. In the two locations studied the following arrangements are in place:

- In *Christchurch* there is a three-tier approach:
  1. Governance is provided by the Christchurch Social Policy Inter-agency Network (CSPIN) made up of senior operational managers from a range of government organisations including, but not restricted to, Police, Education (Chair), Work & Income, CYF, Housing NZ, and Corrections.
  2. A Combined Management Group (CMG) provides the managerial oversight of the initiative, and acts as the interface between the workers and CSPIN.
  3. A co-located group of workers – Police, CPPS, Work & Income, CYF and Health (service provider contracted to the local DHB) – who work directly with the families involved in the initiative.

- In *Papakura* a linear model is used. The initiative is managed and operated by an Interagency Senior Managers Group. Members of the group take personal responsibility for working with identified individuals and their families. Agencies involved include, but are not restricted to, Police, Work & Income, Housing NZ, Education, CYF, and Community Probation. This group has been operating over a six-year period and the POI initiative is one of the more recent aspects of their work. Over this period of time, the group has developed a "*100 per cent total trust relationship with each other*". The ethos of the group recognises the different agendas of each organisation, but work towards the same outcome.

The initiative is also operated in Kaikohe, Flaxmere, Rotorua, and Porirua. In some areas the Area Commander of Police sits on the inter-agency group, but it has been found to be more effective if the management staff involved are mid-managers who have operational decision-making capabilities, and time to invest in working with the clients. For example, Senior Sergeant/ Sergeant level of Police, and area managers of other agencies.

Information needs and requirements

- It is important to know *what information is being shared for* and the *basis for information sharing*. What do we need to know? What is the benefit of joining up with other organisations – to achieve what? In some cases, not all agencies need to be involved. Therefore, officials from those organisations may be party to updates, but not the details. At other times, particular agencies may just not be involved at all. Only agencies that require the information to do their jobs should be at the table. This may require strengthening and using the NGO sector more.

Information sharing practices and procedures

- There is a mandate by management to work together as a single team without institutional barriers to information sharing. This is legal within the context of the Privacy Act: the arrangement is supported by an information sharing protocol developed in conjunction with the Office of the Privacy Commissioner.
- Information sharing is related to the core business of each organisation. Do agencies need to know things for prevention purposes, or are they responsive only? What is the role of NGOs? Who does what/ when/ why? The answer to these questions determines what information can be shared and who it can be shared with. Everything that is needed to be shared is at the table.
- There are two sets of information sharing happening simultaneously – formal (or 'hard') information and informal (or 'soft') information. The latter is based on instinct and judgment; the staff member's consideration of the context in which they are

- There are no management barriers to information sharing between professionals. It is consistent with the nature of co-operation and free exchange of information: that is, 'soft' information rather than 'hard' information is being shared.
- There are different interpretations of the value of informal information (e.g. around offending / drug usage) versus 'hard evidence'. This often depends on the mandate of the agency, and the experience of the staff. The more experienced staff are, the more they understand how valuable informal information can be.
- The nature of the working relationships determines the level of information sharing that takes place. There needs to be confidence that the person being given information has the power and/or ability to use it professionally to achieve the best outcomes for the safety of the individual, the family and the community. Trust in relationships and relationships building is crucial.
- All information is usually done with consent unless there is a situation of life and death. If staff are privy to information which endangers the health or safety of children or others, it is shared regardless of the limitations. These situations are very rare, but: "*pragmatism has to prevail. There is always a balance between ethical considerations and practicality. The broader knowledge we have as practitioners, the more ability we have to help*."
- Information sharing between agencies is done at different levels depending on the role of the agency itself. There are three levels of information sharing:
  1. Across all agencies – what do we know about these families? How is each organisation working with the individual/ family?
  2. Co-location of agency workers who work within existing agency resources, but have a mandate to work with other agencies to achieve better outcomes.
  3. Complex family development models – join up the range of expertise available and produce better outcomes for the family.
- Different models are used in this initiative depending on the region:
  1. Case worker model – an individual coordinates and works with the offender and their family on behalf of the other agencies
  2. Individual offender works with several different agencies all of whom are represented at a local multi-agency group meeting, where a case management approach is taken. Different people take responsibility for particular actions. A tag team is operated if necessary or there are enough resources available.
- POI meetings are verbal. Agencies do not keep records; Police do. Clients can access official Police records at any time.
- Every organisation manages their own information and works within their own agency rules. In Christchurch, the working group is housed at MSD premises in Papanui. A manual working filing system is kept. In Papakura, the Inter-agency Group meets fortnightly for half an hour just to make sure that all the professionals are "*on the same page and aware of all of the key issues*". There is no joint information file; Police take minutes including actions and key information shared at the meeting – who is being dealt with; what is being done; who is taking responsibility for particular actions.
- There is no lead agency in the sense that all agencies contribute equally. Police set the assessment template and get agencies to fill out parts of it in order to determine whether an individual is suitable for the programme.
- Police identify potential participants in the programme. All agencies involved look at their records and decide which organisation is best placed to deal with the person. That is, what are the participant's highest needs (e.g. housing)? A manager from that organisation then buddies with Police and leads the case management process.
- In this initiative families, as well as the individual, give signed consent to share information with agencies and with named individuals/ groups they are comfortable with. The consequences of the information sharing are made known to the offenders and their families before they consent.

- The cultural connection to the family is crucial.
- Service staff usually have the client present and if they need to talk to another agency, they have the client's permission.
- Head office guidelines have been helpful in focusing the programme. Prior to these it was more informal and less focused.
- The agency leading the case work keeps notes on the actions taken, or details of the contact; type of activities carried out (e.g. school uniform assistance); time spent; and agency personnel involved. All of this information is sent to head office on a regular basis. For example, Police provide a monthly report to the Ministry of Justice on progress. At the local level, agencies are unclear what happens to it once it is submitted to head office.
- Police are more willing to share information than other groups as long as it is rationalised around reducing re-offending. The people on this programme pose a risk in one area (offending) and this has long-term effects on the whole community therefore there is a mandate for all organisations to participate.

Information gaps and fragmentation

- There is a definite gap between knowledge of what practitioners do and share and what managers think they are sharing – for practical outcomes.
- Officials are mindful of the constraints around health information. There are some things that they do not/cannot share.
- Health is missing from the table – the problem is that it is a fragmented service at local level. Who do you know to interact with? POI Papakura made a request to Health for representative support. This was escalated to H/O but there has been no response to date. It is sometimes difficult to know where to access health information from.
- Having the ability to involve NGOs would be good as they often have data sets that would be useful. However, there is a lot of government held information that can not be shared with NGOs. Security inside NGOs is not perceived by government officials as being as tight as that within government. The nature of the information held by government can also be sensitive and therefore not suitable for sharing with externals. NGOs often do not send senior personnel to meetings (as they have fewer resources) so they are not seen as taking it seriously. Managers are constrained when not working directly with collegial peers.
- Nobody from Courts participates. It would be useful for other agencies to know about Court hearing dates sooner rather than later in the process.
- Social workers are working with families that have not come to CYF attention – hand-shaking families into NGO services. CYF role could be that of a differential response coordinator. It is currently unrecorded work because it doesn't fit the organisational design structure. Staff involvement requires other people to carry case work loads and this leads to internal professional frustration and resentment.
- In Christchurch, although there is a CSPIN information sharing protocol, organisations often grapple with the issue of what information can be shared, how it can be lawfully shared and why it should be shared. In this initiative the CMG has the task of trying to define the intersection where agencies can share information for the purpose of both individual (including staff) and public safety. The Ministry of Justice POI Information Sharing Protocol has superseded CSPIN efforts. Although an information sharing protocol exists on how inter-agencies should handle information sharing under this initiative, it is often new territory that highlights these issues.

Treatment of sensitive information

- The Office of the Privacy Commissioner and the Ministry of Justice have established protocol rules for privacy protection under this initiative.
- Trust is the key word that determines how sensitive information is shared. That is, trust between professionals and between professionals and their clients.
- Sharing confidential information relies on the trust within the group of professionals and the understanding that information can be exchanged in a professional environment for practical operational outcomes. For example, at one Strengthening Families meeting a new person was uncomfortable about the sharing of names between agencies. Everyone ended up talking hypothetically and nothing practical was achieved.
- There is a code of professional collegial practice which ensures there is "*no come back on individuals for openly discussing any families or individuals*". Managers acknowledge that this practice at the senior management level is different to the messages they present to staff. The explanation proffered for this discrepancy is that it is "*more controlled in a closed environment;[agency] is a 'not controlled' environment*".
- The only information not shared is that from clinical files between patients and their doctors.
- Informal/'soft' information has to be handled carefully. Where professionals act on presumptions based on information they have it could violate the Privacy Act. If the organisation doesn't need it – why have it?
- "*Rights related to an individual's safety and security should over-ride their right to privacy*." By their behaviour, offenders give up some of their 'rights' – not in a legal sense, but in a practical, operational sense. They have to be held accountable. Someone has to say 'enough'. Officials have to share information to get the job done.
- Pragmatism prevails. On occasions staff may inadvertently break the law, but not intentionally. In informal conversations there may be privacy leakage, but information is not necessarily being misused as it is being shared for the purpose of getting the job done and protecting individuals, families and communities.
- Feedback from operational people is that privacy has not been raised as an issue in the field (i.e. by nominated offenders and their families/whanau).
- If it is not appropriate to have something written down a conversation can still take place. Officials operating in the field sometimes "*have to have a blind eye and a deaf ear. There is a need to ensure that what we are doing is legal. Our job is to help families through to a legal position without making it too hard*."
- Professional experience determines where the boundaries are, rather than the legislation. It is important to be aware of who is in the room with you. For example, professionals may not share information about offenders or families if administration staff are in the room.

ICT infrastructure, applications, skills and knowledge

- Each agency has its own secured database. The co-located workers cannot necessarily access their own information from their joint premises. A joint paper-file is kept.
- Security issues arise when staff attempt to access their own databases remotely (e.g. through wireless internet connections).
- The information database is held with the lead agency (Police). It would be difficult if the lead were to change. Having minutes in one place is 'better': "*Even though we trust each other it is still better this way* [that is, held in one place rather than several agencies accessing them]". Minutes are not linked to the Police database.
- Each agency has secured access to limited databases. Everyone has some piece of the whole picture required. People working together can share some pieces of information. Usually email is relied on, which creates a lot of duplication across the system.

- Emails can be frustrating. For example, logos on some departmental letterheads can be blocked by agency firewalls or trapped in SPAM folders.

Barriers to effective information sharing perceived by research participants

- One of the critical issues for all agencies is that of mental health. There are embedded confidentiality clauses in health legislation that govern the treatment of clients, and clinicians think these clauses over-ride Principle 11 of the Privacy Act. In some cases, wrong assessments are made by professionals because of a lack of knowledge in this area. Information sharing would enhance service to the client and improve safety to the community.
- If a person spends less than two years in prison they are often not provided with rehabilitation programmes. Their release time is a high risk time, but release details are not shared with Police. Section 50 of the Parole Act requires Corrections to inform Police *when* prisoners are released, not beforehand. Therefore, Police get no advanced warning.
- Personality issues can be barriers to information sharing. For example, individuals with strong personalities wanted to work together, but couldn't work well together as a team. A broker of power relationships needed to be brought in.
- The biggest barrier to information sharing would be sudden changes in personalities in the job. POI needs continuous relationship building. Once these relationships are broken it is hard and time-consuming to get the initiative back on track.
- Inconsistent representation at management meetings means information is not shared evenly across all agencies. Information between working group and management group can be fragmented when presented to the governance group, and vice versa.
- A joint paper-file is kept, but because of breakdown in trust between the workers, this file does not necessarily accurately reflect information available within the agencies.
- Timeliness of information flow is a frustration. Getting officials together can be difficult.
- More time is required to enable managers to focus on these offenders. At the moment it is done amongst other duties. An inter-agency liaison person would be helpful. It needn't be a Police officer. Their relationship with offenders is not necessarily conducive to co-operation.
- Sharing information is only one part of the puzzle. Bringing people from different agencies together to work on specific projects when at the local level staffing is determined for specific outcomes, is difficult to achieve. Regional specifications are so tight that the ability of individual agencies to contribute to something different is almost non-existent. Government agencies should be looking to re-create/ re-conceptualise how staff are deployed at the local level.
- Staff live in a world of ambiguity where the boundaries are unclear. Managers struggle to understand what is appropriate and this makes it very hard on staff actually doing the job. It is hard for people from different organisations to work together as a team when all around them (management, technology, equipment etc) says they are not.
- No-one wants to give up resources to accommodate [Head Office devised] joint initiatives because local resources are so scarce. MSD has the most flexibility. There is scrutiny from H/O and MPs because they want joint outcomes, but they are also very risk averse so it is very hard for some of these initiatives to operate because they are working on very risky ground.
- The central support from H/O in terms of providing funding, resources and management of the political pressure is not forthcoming. There is no sense of direction from the centre. Regional managers have the imperative to make inter-agency initiatives work, but there is a high investment with not much outcome.
- It gets too hard without central direction. There is no level of autonomous decision-making to do particular things. Each Regional Manager is likely to get into trouble for

- Legal people in each agency, especially in relation to information sharing and privacy, need to be talking off the same page: there are different interpretations of the Privacy Act coming from different H/Os. Which interpretation needs to prevail in cross-agency collaborations?
- It is difficult when an external group (e.g. members of a local marae) is not privy to the privacy consent that the individual has signed as part of the process. Individuals may give separate consent for externals to be involved for specific purposes only.
- There are problems around storage and ownership of shared information. For instance, how does information get stored when staff are co-located but come from different agencies? Does each person carry their own memory sticks: where does that information get stored? How do Police, Probation, or any other agency personnel access their own databases when they are in an MSD building, and possibly using MSD equipment?
- The original family trees [that the initiative is based on] are not being updated and monitored.

Enablers of information sharing perceived by research participants

- Trust in relationships and relationships building between agencies is crucial.
- The initiative could use a shared database contributed to by different agencies. Access could be covered by protocols and authorities.

Case Study Area 5: Electronic Monitored Bail (EM Bail)

Programme	Short description
Electronic Monitored Bail (EM Bail)	▪ Ankle bracelet monitoring system for persons awaiting trials. Purpose is to reduce the number of people held in prisons prior to trials taking place. ▪ NZ Police personnel assess applications for EMBail by individuals awaiting trial. ▪ Liaison takes place with Housing NZ, MSD, CYF, Health, employers, and Work & Income to assess whether a person is safe to be released into the community and how the bail conditions will be met. ▪ Types of information shared include offending history, personal details and service needs. ▪ Approximately 120 people are currently on the programme and it is operating in every Police District in New Zealand.

Background

EM Bail is applied for by remand prisoners wishing to spend their pre-trial period at home with electronic monitoring. This allows "*eligible defendants to live at home or an approved community address, wearing an electronic bracelet as part of their bail conditions*" (FAQ – NZ Police website). The electronic bracelet sends a continuous signal to a monitoring unit linked to a control centre which monitors and records the person's movements 24 hours a day. EM Bail does not stop the person leaving the designated area, but if their departure is not pre-approved an alarm is raised which is responded to by Police.

Authorisation is given to NZ Police by the applicant via a signed consent form to carry out comprehensive checks on the individual to ascertain their suitability for the programme. Police act as the single point of assessment, but obtain and share information on the individual from a broad range of agencies and individuals within the community (e.g. employers, family members). The information received is used to compile a report for consideration by the Court on the suitability of an applicant to remain at home until their court hearing. Fifteen working days is allowed for information gathering, site visit and the presentation of a report to the Court.

In granting bail a Judge has to take into account the likelihood of further offending, absconding, interference with witnesses, the seriousness of current offence, previous record and behaviour, and the safety of residents, applicant, victims and the community (s. 8(1)–(3) Bail Act). EM Bail Assessors (i.e. Police personnel) have to present a balanced risk assessment of the likelihood of any of these events occurring and provide the Judge with evidence based information where possible. Currently the national policy is that if a 'significant risk' can be demonstrated then the applicant remains in custody.

Once a person has been granted EM Bail by the Court, the Bail Assessors have responsibility for arranging the process. The electronic bracelets are supplied and monitored by a private company (CHUBB). The EM Bail Assessors have responsibility for monitoring all pre-authorised leaves of absence from the premises (e.g. medical appointments; education or employment arrangements).

Information needs and requirements

- At the moment, agencies receiving information requests are responding according to their perception of what is needed.
- Priority is about getting information that enables an assessment of the safety and the security of the placement, not about re-offending.
- A technical assessment is carried out to ascertain if a signal is available. That is, can the electronic process be physically put into place?
- National statistics on the programme are collated and distributed on a weekly basis to "*everyone who has an interest*". This summary is provided on a spreadsheet and distributed via email. It is used by management staff to identify pressure points in the district and ensure resources are appropriately distributed. Once a year, the information is collated into an annual report.
- Internal communication is an issue. In smaller areas, there is a weekly update for station staff and a District roundup / briefing on application processing; EM Bail breaches; terminations. In bigger districts, this is not practical. Even if it was put on the District Bulleting Board, it may not be read.

Information sharing practices and procedures

- Principle 11 of the Privacy Act authorises sharing of information for safety and security of the community. Managing risk is the full purpose of sharing information on this programme.
- It is a judgment call about information that can be shared. There is a mixture of information the Assessors are obliged to share with particular people (e.g. current/past offending history with the other occupants of the residence) and what people need to know. Assessors are very conscious / sensitive about releasing information on a 'need to know' basis without compromising the privacy of the bail applicant.
- Assessors are given two types of information: (i) '*we will tell you this, but you can't use it*', and (ii) '*we will tell you this and you can use it in your report*'. Some information cannot be reflected in the way it was delivered without losing the importance of the content. Assessors try to protect people, but also to provide facts for the Judge. "*There is a difference between 'evidence' without knowledge, and 'knowledge' without evidence about someone's circumstances. Assessors have to make judgments about what can be provided in official documents*". Recorded ('hard') information is done with a consciousness of how it will be used and who will see it.
- As a general rule, the less formal, the fewer restrictions there are on sharing by individuals. The more formal it is, the more risk aversion there is. People have to check at their own end what can and cannot be shared. Everyone is initially cautious. No one wants to be responsible for sharing information they are not legally allowed to. Most agencies are conscious of their responsibilities under the Privacy Act. There is also a strong fear of being caught and being subject to retribution from individuals and organisations.
- In some cases, some information is shared on trust that it will be used appropriately. People do not have the authority, but share anyway. There is quite a bit of "*off the record*" chat.
- Facts do not always add up and make sense. Some information is not relevant to the bail application but is still relevant for an individual's personal safety. For example, Probation informed the Bail Assessor in one case that "*we had to change his Probation Officer because he was making sexual passes at her*". Such information allows the Bail Assessor to make a judgment about the safety of other people who may be sharing the residence with the applicant.

- Assessors do not speak to the applicant at any stage of the process.
- An application includes a consent form signed by the applicant for Police to gather information from a broad range of informants including City Council, Court (Judge's notes), Prison, Community Probation and Psychological Services, nominated health providers, training facilities and/or schools, rehabilitation and/or reintegration facilities, employers, residence facilities as well as Housing NZ, CYF and Work & Income.
- All applications go to the EM Bail Programme Manager in each Police area and they are then distributed to the Assessors in the district. Final sign-off on the reports is made by Area Managers before they are sent back to the Courts.
- The information gathering process is a standard desk-file process. Each step has process forms (template) which are faxed to agencies for completion. Information requests are sent along with a copy of the signed consent form.
- Much of the material gathered is by means of staff from relevant organisations filling out templates requesting information on the applicant. Most external agencies respond reasonably well once they understand what it is about. Some home visits and/ or face-to-face meetings are carried out with family members and employers. It is in the best interests of employers to share information therefore they are usually very cooperative.
- Each organisation has to interrogate their databases. Sometimes Assessors get the wrong information. Information needs have to be re-clarified and the information double checked.
- In lots of cases the information gathering process depends on personal relationship management. Some agencies have individuals who are brilliant at assisting with the monitoring process. For example, WELTECH has set up a contact person who has a direct line to the EM Bail Assessor and provides information as required. CareNZ sends notes of attendance to the Bail Assessor as a matter of course.
- An on-site assessment is made of the premises where the applicant intends to live and the residents there are interviewed. This enables the assessor to make a judgment about the suitability of the living arrangements, but also provides them with an opportunity to ensure that the people who will be living with the applicant, are aware of any issues relating to the applicant and his/her social circumstances.
- Assessors need to provide information to the occupants on the EM Bail programme and what it means. They may also share information on the nature (but not the details) of the current offence and the applicant's offending history so that the occupants are fully informed before giving their consent (by signature) to the process.
- Assessors are careful about what is divulged and to what extent. The 'need to know' judgment is used as a rule, based on the need for safety. Usually Assessors ask people to "*tell me what you know*". They will then add or correct information if necessary. Assessors are aware of their personal accountability for what is revealed.
- Occupants of a residence can be hesitant at first: "*Once you set out the ground rules of confidentiality they are more relaxed, and the more they tell you. If there is something to hide you soon pick up on it*."
- EM Bail Assessors end up being social workers – trying to liaise with government agencies to ensure that the conditions of the bail are put into place. Variations to bail conditions go through lawyers but can fall back on Assessors although it is not technically part of their job.
- A degree of chase-up is accepted because of the processes that are currently in place. Delays are part of systemic issues.
- Assessors cross-check with Intelligence section before making site visits. They need softer knowledge about any operations underway: a heads up is needed for personal safety. For example, it is wise not to visit sites alone on the first occasion until you know what you are getting into. Go with other Bail Assessors or front-line staff.
- Private organisations are generally very quick in providing information and often provide more than is required. This is because the Police are regarded as official agents and a trusted source.

- If an agency opposes the application, they are more likely to commit it to writing. Less is written if there are no concerns.
- During monitoring and/or if additional relevant information is found out (e.g. psychological history), there is an opportunity to seek an early Court hearing and return or revoke an EM Bail provision.
- Administrative requirements at each end of the process cut the actual time for gathering information down to 10 days actual time (e.g. management sign-off; reports have to be back in the Court 2 days prior to the hearing).

Information gaps and fragmentation

- Requests are standardised nationally (i.e. via template) but there is no national process between agencies for the information gathering process.
- Sometimes it is difficult to work out with some agencies, which Service Centre (e.g. Community Probation) does what. They are separated according to an internal system that is not immediately apparent to the external person. It is difficult to figure out whom to ask for the information required.
- Some Police are unaware that EM Bail is run by the Police. In big geographical areas it is hard to get proper internal information. People associate EM Bail with Home Detention run by Community Probation. The differentiation is not being understood internally. Even the Communications section always need to be told it is a Police run programme.
- The monitoring role also contributes to the perception that EM Bail Assessors are not Police personnel. The Communications Centre staff members sometimes hold information on breaches over for the weekend to be referred to Community Probation even though it is the Police who are supposed to respond immediately. The only operational duty Police have is to attend to breach notifications. Once breaches have occurred it goes straight back to Court and is no longer a Police issue.
- Front-line Police and EM Bail Assessors have different expectations about who monitors the bail applicants and why (e.g. who makes the decision to arrest for breach?).
- There are boundaries around official information sets which mean that different professionals know different things that may have a substantive impact on the final report. For example, CYF may have no issues with an address (i.e. they are not aware of any offences against children occurring at that address) and formally sign-off on approval of the bail application. However, the offender may have a previous history of domestic violence in front of children and therefore may not be suitable for placement in a household with children. If CYF had been aware of this information they may have changed their approval recommendation.
- CYF identifies risks to children in the residence based on historical records. The current offence is not relevant unless it directly involves the children.
- Current recorded data does not carry the level of detail needed to provide relevant links and tie it all together. For example, who acted for the person at the EM Bail hearing? Moreover, what were proposed addresses, or information about social circumstances? Incomplete or incorrect information can have knock-on effects for the bail applicant, victims, family, or other members of the community.
- More detailed information sets from agencies are required to formulate a factual report to the Court: "*Yes, it's fine and feasible*" doesn't help.
- If information about an address cannot be checked (because residents cannot be contacted on site) the Court and the applicant's lawyers are advised and a request is made for another Court date for a different address. There is no feedback loop on this event.
- Not all agencies are responsive to the information gathering process. In some cases, internal processes are complicated and this results in non-performance and/or there is a

- Agencies work on the basis of different information sets and requirements. For example, quite often the information that comes back from Housing NZ cannot be used by Assessors. There is a requirement that they be notified, but a lot of the information they supply is not relevant to the EM Bail application. The Housing NZ view of who they want living in their residences is irrelevant to the application unless it has a legal basis (i.e. in the Housing Act). It is not their decision, and unless there is some regulatory or legal impediment to the applicant residing in one of their properties, their input is not helpful.
- There is limited contact between Assessors. As a result, opportunities for learning transfers are restricted.
- Local practice varies from national standards (e.g. protocols surrounding site visits).
- If a bail applicant is living in the Hutt but the charges are in Wellington there is a problem. All variations in the conditions of the bail arrangements have to be physically dealt with in the Wellington office because the Hutt staff refuse to deal with Wellington cases. By contrast, Auckland central Bail Assessors report that if the planned address of the bail applicant is outside of the Auckland central district it is dealt with by the local Bail Assessment team and reported back to Auckland central.
- There are problems getting information within the very short time frame required for the EM Bail application process (15 working days). External organisations do not meet the required timeframes and Assessors spend a lot of time chasing up for information.
- Both the quality and quantity of information possible to obtain is compromised by tight timeframes. There is pressure from lawyers for 'quick hits'.
- Probation Officers can be "*too busy to talk to you*", which leads to more work for the Assessors. They are bound by other people's processes. EM Bail can't dictate other organisations timeframes and they may not care about Police/Courts timeframes. There are often apologies because people are overworked and the information requirements have been overlooked under other priorities.
- If information from agencies is not forthcoming in the timeframe available the only choice Assessors have is to advise the Court that "*whilst reports were requested, they have not been received*". No advice can be proffered without information. If information is important and Bail Assessors have been advised of a specific hold-up they may seek an adjournment from the Court. This is a particular problem too with Judge's notes. Judges won't make decisions without checking their previous notes, but if these are not made available to the Assessors by the Courts, they cannot be included.
- Courts reply to requests eventually but not in a timely manner. There is trouble locating files between offices of the Court. Similarly with information from the prisons. Sometimes information doesn't come at all and sometimes it comes too late. Information received may not be relevant, but you cannot say it won't be useful if you do not have it.
- Sometimes it is hard to get hold of the Criminal Court Registrars as they are especially busy.
- Risks to the applicants are advised to the Court, but not necessarily to other people interviewed.
- Variations in practice between local districts are not transparent and poor information transfer about changes in process (e.g. Court adjournments) can create inefficiencies.
- The 'business reports' generated as a sub-programme of the mainframe do not deliver a national picture and report the types of data required by politicians and the media (e.g.

- Probation also uses electronic equipment and has a monitoring relationship with the same company. CHUBB reports indicate that another anklet (HD) is on the site, but will not provide details. Liaison has to take place to check violations. The privacy emphasis is on the provider.

Treatment of sensitive information

- Regardless of the agency – if there is a personal safety issue professionals feel a moral obligation to ensure other workers are safe. For example, being warned that there is someone with HIV who is a 'spitter'.
- There is no avenue to share some confidential information; therefore it is shared within 'professional confidence'. Informant information sometimes cannot be acted upon although it is relevant because it cannot be 'proved'.
- There are no rules to allow for the sharing of personal information so workers 'work around' it at the risk of getting into trouble for it. Assessors work in a world where confidential / private information is known, but can only be used in a limited way.
- Potential concerns about privacy are offset by the applicant's signed consent to the programme. However, if lawyers cross out authorisation of particular sections of the assessment (quoting privacy or contributing to investigation at a later stage), then the assessment cannot be completed and the Assessor has no choice but to advise the Court of that.
- Information sharing on individuals is very rare at the national level. It is usually not necessary to do the jobs required at that level. The application form authorises operational people to check information, and to give out information to agencies. There is a question as to whether this level of authorisation is necessary for this programme. Exemption provisions may enable information sharing anyway.
- There are difficulties with getting information from health providers because of confidentiality and privacy concerns. The EM Bail Assessors are not interested in the person's health matters, but they do need to know if the person has physically turned up for an appointment and when they leave the premises. They also need to know any associated care needs that will impact on the person's bail conditions (e.g. need to attend out-patient clinics for regular treatment, or one-off treatments). The best practice is to make contact with a particular person in the doctor's office and establish a professional relationship. If they understand the programme they will assist and the monitoring process runs well.
- There is a major problem for Assessors to obtain mental health information needed to explore whether treatment or care requirements can affect ongoing monitoring or physical care arrangements. Mental health providers are very reluctant to provide that information. Front-line staff need internal permissions to release information.

ICT infrastructure, applications, skills and knowledge

- EM Bail is one of the initiatives in a broader sector strategy around effective interventions. Although data on the programme is shared with the Ministry of Justice, the Case Management System (CMS – MoJ system) does not record the depth of data needed for Police to manage the business. Police are creating an increasingly large spreadsheet with more detailed data. The long-term intention is to get the information into the Police computer system, but there are other technical priorities at this time for Police.
- Assessors have no access to databases of other agencies.

- Access to internal electronic systems is not a problem, but there is no way of knowing if the data is up to date or reliable, or even still relevant. Summary of facts and other case material may be incomplete. Victim impact reports are on the physical file, but may not yet be on the electronic file.
- Access to information from Police personnel is problematic because of a lack of understanding of the programme.

Barriers to effective information sharing perceived by research participants

- The single biggest barrier is a lack of understanding of the programme. People need to know it is a Police operated programme and a pre-trial process: therefore, it won't affect the outcome of the subsequent Court process. There is a lack of knowledge about the difference between Home Detention (HD) and EM Bail. For example, Work & Income staff assume that (as in HD) an offender can attend their office at the Probation Officer's discretion. However, this is not the case with EM Bail. Unless it is already known that an offender has to attend a Work & Income appointment, they are not free to go to the office. Any variation to the bail conditions has to be made by a Judge. Consequently, this has to go back to Court and this takes time: "*It is a constant battle to educate Work & Income about something that is not part of their core business*".
- It can be difficult getting hold of the Officer in Charge (OIC) of the case, especially if they are at Constable level and often not in the office. They can be on different shifts, or on leave. Sometimes they have a perception that the EM Bail Assessors are from Community Probation, and they won't co-operate with them. Often the OIC won't return phone calls or respond to emails (even when it is apparent it is from an internal email address). They have no 'out of office' details and simply do not respond. This is particularly an issue if they oppose bail and they believe that the EM Bail Assessors are working against all of the work they have already put in.
- There is a perception by some Police staff that Probation staff are not professional. They have no trust that 'their' information is going to be safe and therefore they do not co-operate with them.
- If Police evidence is strong for an offence, and they have a view of the offender and the appropriateness of EM Bail, this is important to share with the Bail Assessors. However, Police see the process as one that undoes all of their hard work and therefore are reluctant to share important information. The Police Prosecutions section work hard to ensure a person is put in custodial remand in the first place; therefore, there is an internal conflict of interests between staff within the same division.
- There is hesitancy on the part of officials to get 'caught up' if information is formalised. For example, CYF personnel may get called to Court to discuss information they may have provided for the assessment.
- EM Bail has no legislative status. It needs a more legal standing: for instance, enquiry forms are only guidelines; they are not compulsory and some agencies only respond to them on a discretionary basis. The checks and balances in the process are not adequate.
- Difficulties in obtaining information are a result of (i) work overload, (ii) ego – do not want to share information or 'ownership' over information sets: too important to share, (iii) different interpretations by different professionals, (iv) the profile of EM Bail is blurry and not strong in definition.
- Information sharing between agencies is not addressed in specific legislation to streamline processes.

Enablers of information sharing perceived by research participants

- In the longer term, the programme needs to specify more clearly what information is needed. For example, Housing NZ's 'opinion' of the placement is not required, or important to the final report. What is required is information about whether the

- Information request forms need to be more specific about what each agency needs to contribute. For example, CYF needs to be asked to check the address; check the offender; and match the information against each other to give an accurate risk assessment.
- The process works most efficiently when each agency has a central point of contact, and a person to work with.
- Work & Income (Steps to Freedom) set up processes between one person and the Bail Assessor. This saves management issues and ensures that barriers to providing bail applicants with income support are overcome. The Work & Income processes tend to be inflexible, which doesn't accommodate the programme and leads to greater compliance complications. Different areas approach it differently.
- Even if Assessors could view databases of other agencies, but not have authority to change them, it would save time and reduce duplication of information and effort.
- Access to broader information sets would reduce the need for human judgment factors that multiply across information sharing processes.

5. Cross case study analysis

The case studies examined in this research varied widely in their purpose, the agencies involved, and the information sharing arrangements used. They were similar only insofar as each was working with clients with multiple and often complex problems, the resolution of which required input from a range of government and non-government agencies. Across the case studies however, the following 'patterns' of research findings could be observed:

Information is shared on a 'need to know' basis

Across the case studies we could observe that information sharing between professionals of different agencies is happening, albeit not in an open or unrestricted way: information is shared on a '*need to know*' basis and justified in terms of ensuring that people know enough to do their jobs effectively and safely. Professionals are conscious about the need to protect personal information, but apply '*common sense*' in cases where that protection of personal information might stand in the way of the protection of professional, personal or community safety. In those cases, abstracted information is often used to alert other professionals about the need to further investigate a particular client.

Information sharing is strongly related to trust in relationships with other professionals: without that trust, information is not shared.

All case studies provide strong evidence for the fact that information sharing is related to the trust that a person giving the information has in the person receiving the information to treat it professionally and use it judiciously. Without that trust, information is not shared. That is, the professional role or organisational status of the individual (e.g. Police Officer, Team Leader, Case Worker etc) will not necessarily ensure that relevant information is passed on to another professional from a different agency, or even to a colleague from the same organisational unit. For instance, if other professionals do not trust that individual, based on either their professional behaviour (e.g. has displayed poor judgment in the past) or their organisational status (e.g. a Probation Officer and therefore an outsider to the Police), then information is with-held or presented in a minimalist way. Examples of this include the difficulties EM Bail staff have in obtaining case information from Police Case Officers: they are perceived to be working for the Probation Service and are therefore 'outsiders' and not entitled to 'police' information. Under the POI programme, this was also demonstrated when some of the case workers expressed no-confidence in their CPPS colleague and therefore did not share information with her unless absolutely necessary.

On the other hand, where professional trust is high, professionals with different mandates (e.g. Police, Work & Income staff, Probation officers) share information openly and beyond that which is required by the official parameters of their specific job. With that, we may conclude that the quality of information sharing depends on the quality of relationships between individual professionals. However, we can also observe that the quality and quantity of information sharing between professionals from different agencies is further increased when there is a clear commitment to a shared outcome (e.g. POI in Papakura; HR/HP initiative in Christchurch).

Professionals use different information sets according to their core business needs

Information relevant to achieving the shared outcomes being sought in the initiatives under study is <u>not</u> homogeneous in nature, but involves a wide variation in information

needs of different agencies as well as different policy sector-related information sets. For example, Work & Income may only need to know a person's current status in relation to a range of variables, such as marital status, number of dependent children, current address, and/or offending record (i.e. have they recently been released from prison?), in order to establish their eligibility for specific benefits. For other agencies, such as Police, CYF or those providing health services, alterations to an individual's status and living arrangements over time may be important to assess their level of current need, relevancy of services, or the degree of risk they pose to others depending on the circumstances of the interaction.

Professionals use different interpretations of 'valid' information

The fact that agencies have different information needs and requirements also leads to a situation in which different information sets are regarded as 'valid' by officials from different agencies, affecting how information is processed and used. Officials make decisions about the validity of information and therefore what they can act on, and what is disregarded as unnecessary to the completion of their duties. For example, a Probation Officer may have to decide whether 'intelligence' information that a particular residence is being operated as a 'P' house is relevant in the absence of hard corroborating evidence and therefore can be taken into consideration in assessing the suitability of that address for placement of an offender on parole. Similarly, a Work and Income official may not regard previous criminal offending relevant to making an assessment about current benefit eligibility.

Such judgments to act upon, or not act upon 'invalidated' information have implications for officials and/or the community. If information is irrelevant to the mandate of a particular official do they need to have access to it, or take it into account? Is there any ethical imperative to do so over and above the operational technicalities of their official task? Where different officials are co-located and working towards the same outcome what are the boundaries relating to information sharing where different participants have different information needs? The resolution of these questions can be critical to the quality of service delivery and to the practical implementation of official's 'duty of care' to individuals and the communities which they serve.

Furthermore, there can be situations in which officials and their clients have different interpretations of the agency's information needs and requirements. For example, in the case of the Refugee Service Organisations, we could observe that information requirements of government agencies clash with the cultural norms of refugees. This particular example reveals that who does what with the information, is as important as the information itself.

Signed consent forms are used by professionals as authorisation to share information

All of the case studies we examined have clear documented processes whereby individual clients consent to particular sets of information being shared across agencies and amongst professional groups. These consent forms vary in detail and depth. For example, the EM Bail applicants sign consent forms that enable Police Assessors access to a wide range of personal information, and enable them to share that personal information with other officials and people nominated by the applicant. On the other hand, the consent forms used by agencies providing services to refugees are very broad and general. In all cases, signed consent forms are used by officials (government and non-government) as authorisation to share information on the client's behalf, and to share information about

clients with other professionals (and in some cases people associated with the client) as necessary to achieve their organisational goals.

Professionals make a distinction between formal or 'hard' information and informal or 'soft' information

Across the case studies we could observe that front-line staff make a clear distinction between the following types of information:

- *Formal or 'hard' information* – that which is written and exchanged through formal processes between different professionals, between professionals and their clients, and between officials from different organisations (e.g. exchange of papers, fax, emails, templated information held on a database). Often, formal information is reduced to core facts with little associated substantiating evidence.

- *Informal or 'soft' information* – that which is unwritten and exchanged usually directly 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.

Front-line officials therefore operate in a situation in which they not only are making judgments about the validity of information, but also are assessing whether they can use that information officially, or if they can act on it unofficially. Moreover, they make judgments about what information can be shared with whom, and for what purpose. In this respect, respondents indicated that a clear distinction is made by officials between information that can be committed to writing as part of the 'official record' and information that can be acted upon. As one respondent further explained: "*there is a difference between* '*evidence' without knowledge, and* '*knowledge' without evidence about someone's circumstances. Staff have to make judgments about what can be provided in official documents".*

There is evidence from several of the case studies that professionals are exceedingly particular about what is officially recorded with respect to any individual, and there is every likelihood that the written record only constitutes a small percentage of what officials 'know' about an individual and/or about a situation. It is the combination of 'hard' and 'soft' information which forms the basis for professional judgments about operational practices on a daily basis.

Professionals relied more heavily on 'soft' information

Officials indicated a particular awareness of how official records can be, and often are, used by different parties for different reasons (e.g. lawyers, media, and in some cases the clients themselves). In this respect, several professionals indicated that they rely more heavily on the 'soft' information or "*what we know*" as opposed to the official record. There was a clear indication from the interviewees that this approach provide a number of distinct advantages to officials with respect to their personal and professional 'safety' and the safety of other people.

Professionals ensure that colleagues know enough to do their jobs safely and effectively

Across the case studies there is strong evidence of an implicit professional code amongst officials relating to the protection of professional, personal or community safety. This

professional code of safety protection operates in both formal and informal processes and is extended to other service providers (government and non-government) and members of the community. For example, an agency providing residency for prisoners on their release may be informally alerted to possible issues that may affect the safety of their staff or other residents. Similarly, as part of the formal suitability assessment process, EM Bail staff ensure that other residents in a property where a person will reside while on bail, are aware of any previous offending before they give their consent for the person to be released to that address, so that they are making an informed decision (albeit without supporting details). A further example is when a person has a mental health problem and the details of this problem cannot be shared with other officials, the health professional concerned may indicate to other staff (e.g. prison staff, case workers) that the individual needs a particular medication regime, thereby signalling to staff that this client has a different set of needs compared to other people they are dealing with.

For those agencies working under a public safety mandate, where community, professional and personal safety is a paramount issue in an operational sense, respondents indicated that they see '*Principle 11*' of the Privacy Act, 1993 as enabling them to share critical information with other professionals and, with that, as the embodiment of this professional code. While Principle 11 was regarded by respondents as enabling them to share critical information, they were also clear that this is only done on a 'need to know' basis amongst professionals attempting to achieve the same outcomes. In this respect information sharing that included personal data of individuals, is not seen as a violation of privacy but as something what has to be done to 'do the job effectively'. In other words, there was a view that some jobs involve the sharing of personal details in order to do these jobs effectively. Privacy was not regarded as being violated by personal information being shared with officials who have a role in relation to that person.

For agencies working under a public service mandate, where public safety is not dominant in an operational sense and therefore Principle 11 of the Privacy Act, 1993 was not applicable, we observed that the same implicit professional code of safety protection is applied amongst officials. Although, in principle, personal information on the client is confidential, this principle may very well be ignored if the staff member judges that there are professional, personal or community safety risks: in those cases, critical information is shared with other professionals on a 'need to know' basis. For example, a Work & Income assessor is aware that a client displaying problematic behaviour as a result of a drinking problem is on his way to another agency and informs a representative of that agency that a client with a health-related issue will arrive with them soon. Several respondents explained that, from their perspective, '*common sense needs to prevail'* in these situations. Acknowledging that there may not be a legal back-up for their decision, one interviewee further clarified: "*If staff break the law, they do it for the right reasons*".

In general, interviewees indicated that they do not 'gossip' about their clients, but neither will they allow other staff to unknowingly be put into positions that constitute a risk to that person.

There are clear differences in information sharing practice and procedure between agencies with a public safety mandate, and agencies with a public service mandate

Where agencies with a public safety mandate use Principle 11 of the Privacy Act, 1993, for sharing critical information with other organisations, agencies operating under a public service mandate do not have such a legal 'back-up'. For agencies with a public service mandate, this leads to unclear situations of where the (legal) boundaries are with respect to the sharing of critical information with other agencies. This applies to the sharing of critical information both with agencies operating under a public safety

mandate, and with agencies with a public service mandate. As public service staff experience uncertainty about whether, and if so what information can be shared, the default position of staff is not to share information.

This default position of not sharing information leads to situations where there is no sharing of 'intelligence' between agencies (e.g. between Refugee Service organisations about shared clients; between Corrections and Work & Income about system 'rip offs' in the area of income support); or where agencies focused on their own agenda are not meeting the holistic needs of the client, which, from a client's perspective, can lead to flow-on complications with other parts of the system (e.g. in the case of refugees: not meeting eligibility criteria for income support has implications for housing).

In cases where critical information sharing is not happening, professionals are sometimes being exposed to danger without their knowledge (e.g. a female official from a service providing organisation not knowing that an inmate has a criminal history of assault on female officers).

In the case of the Linwood Service Centre, the default position of not sharing information and the lack of a legal back-up for sharing critical information leads to a situation where clients need to join-up service providers, so that their complex needs are being met: as clients need to pass on the referral form to the agency concerned, they control the information provided to the various partner organisations in the Integrated Service Response initiative.

As a result of consistently using signed consent forms as an authorisation from the client to share information on their behalf, several respondents indicated that issues around privacy protection are not so much emerging in relationships with clients, but in relationships between organisations. For instance, due to perceived risks in decision making around privacy legislation, public service staff are often overcautious with applying the Privacy Act in relationships between organisations and therefore not wanting to share critical information. An interviewee observed that "*the Privacy Act slows down quality services targeted at clients with complex needs and with the right intentions*". Some respondents also reported that staff hide behind the Privacy Act (HR/HP) as a reason for not doing something.

There are strong boundaries around particular data sets, with strict protection by authorised personnel

Across the case studies we could observe that particular data sets, such as medical records and child protection records, have special protection: access to these data sets is only allowed for authorised personnel, i.e. professional experts in the area concerned. Moreover, certain sets of information, such as details of physical health, mental health or criminal histories, are bound by legal constraints and therefore are not shared even amongst professionals. These particular data sets are recognised by all professionals as outside of bounds, and there is no indication from any of the case studies that details of these records are ever subject to sharing. While all respondents were accepting of the need for strict privacy around personal health issues, this was also the area that was unanimously reported as posing substantial difficulties in an operational respect.

Health information is not shared, but critical information in this area is often required to do a professional job

Respondents reported that the difficulties obtaining medical information is the area in which they are most exposed, and in which safety issues for them personally and

professionally, and for members of the public are most likely to arise. For example, refugees experiencing various forms of post-traumatic stress disorder can pose problems to themselves, their families and members of the community as well as the professionals tasked with providing them with services and assistance. Without knowledge or information on the health-related factors involved in any given situation, officials are compromised in their ability to protect individual clients, members of the community, or even themselves.

Interviewees also provided examples where health-related information was not shared between professionals, which compromised the individual from receiving services they were entitled to. For example, a refugee continuously missed appointments and when a home visit was carried out they turned out to be a double amputee whose physical ability to participate was compromised and who needed special support that the providing agency was unaware of.

Furthermore, several respondents reported that many health practitioners were unwilling or unable to co-operate with other professional organisations (government or non-government), 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). In this respect, information sharing practice was widely variable and depended almost entirely on the attitude of individual practitioners, the interpretation of local administrators as to how they should be applying the Privacy Act, 1993 (i.e. what information they could and could not share), and the ability of officials to build working relationships with other professionals and across agencies. There was no common understanding of how the Privacy Act, 1993, should be applied in these health-related information sharing instances across agencies, and no common practice.

Respondents also noted that, as the health sector is fragmented and widely distributed, they were often unclear whom to invite to the table, or whom to contact in order to obtain information with respect to individual clients.

Information sharing protocols are useful for establishing effective information sharing

Respondents reported that having an information sharing protocol in place has helped to develop relationships with officials from other agencies and build trust. Moreover, compared to the situation prior to having the information sharing protocol, it has helped to bring officials from different agencies around the table. Another advantage of having an information sharing protocol is that it provides clarity to officials about how to interpret or apply legal provisions.

In case studies where an information sharing protocol is in place, we observed that professionals treat each other as colleagues even when someone is employed by another agency – for the purpose of the initiative, they are treated as 'honorary employees' privy to the same information sets. For example, Police members participate in HR/HP meetings with Corrections staff and share information about inmates, as well as receive information. Similarly, the senior managers involved with the Papakura and Christchurch POI initiatives share agency-specific information across agency boundaries in the interests of ensuring that they make informed decisions as a group about the suitability of any individual for the programme.

However, in the information sharing protocols under study, grey areas around information sharing with community-based service providers can be observed (e.g. NGOs). For example, government agencies often have formal information sharing protocols between them, but many other organisations assist with practical needs; it is unclear to

professionals concerned how much can be shared with these community-based service providers, and how the Privacy Act, 1993, can be interpreted around that. In the cases under study, a consent form often overcomes these problems.

Co-location supports information sharing practice

Several respondents reported that co-location enhances opportunities to develop relationships with other agencies, build trust amongst professionals and, with that, share information with other professionals, for instance in cases where there is no information sharing protocol in place. For example, at the Linwood Service Centre, co-location of government and non-government agencies means there is information available that otherwise would not have been shared between these groups: new shared records are being created which can be accessed by all agencies on site. Although these are paper-based, the status and quality of these records is questionable: for instance, who 'owns' these records? Which agency (if any) has responsibility for managing them, ensuring their security and accuracy and/or ensuring they are covered by disaster recovery procedures?

In general, there are serious questions about the completeness of records held on 'co-located' sites, and their usefulness. For example, respondents indicated that Linwood Service Centre workers rely on processes of other agencies, such as filling out and signing of information sharing consent forms, without actually physically checking on the shared paper records that consent has been given. In the same vein, respondents pointed out that, under the POI initiative in Christchurch, because of a breakdown in trust between workers from different agencies, the records held on-site did not accurately reflect the information that is available to officials from their agency databases.

Officials use manual 'work-around' techniques to compensate for a lack of technical interoperability of information systems, or no access allowed to personnel from other agencies

Each agency has its own information storing process. Police, Corrections, Courts, Health, Work & Income, CYF, Education, and presumably other individual agencies, all have secured databases containing information on individuals pertinent to their own mandate. Access to these databases is restricted to agency personnel only. This not only implies that each agency has fragmented information relating to an individual, but also that officials use manual 'work-around' techniques to compensate for a lack of technical interoperability between information systems belonging to different agencies, or for the fact that access to these systems is not allowed to personnel from other agencies. These manual 'work-around' techniques involve duplication of data and data entry processes, as well as sending and receiving emails with sensitive data in attachments. For example, because Police personnel participating in the HR/HP initiative cannot access the Corrections Integrated Management of Offenders System (IOMS), relevant information is sent to them on excel spreadsheets, which they have to manually match against the Police databases. The spreadsheets are then updated in the spreadsheet manually by the Police and sent back to Corrections, where an administrator cuts and pastes the additional Police updates back into IOMS before the HR/HP meeting.

Where officials from different agencies are co-located (e.g. POI Christchurch) paper-based files are assembled because no shared database is available that personnel from a range of agencies can access. In other cases, shared databases have not yet been established for some initiatives, especially where cases are operating on a pilot basis. In a few initiatives, core information is shared via Excel spreadsheets (e.g. EM Bail).

Case study findings also indicate that some of the cumbersome information processing taking place is due to the lack of technical interoperability between government agencies, or between government and non-government agencies (e.g. Linwood Service Centre, POI, HR/HP, and Change Makers). This interoperability is partly an issue of incompatible operating systems (Linwood Service Centre, Change Makers), but in some cases it is directly related to information security issues (e.g. access restrictions) or issues around the ownership of information (e.g. 'controlled' databases).

Technical solutions for improved information sharing are available, but unused

In the majority of the case studies, technical solutions to the management of information sets across agencies were available, but unused. Explanations for this situation varied from officials being unaware of the technical support options available to them; agencies lacking the technical capability to explore and use technical solutions available to them; to a desire by some officials to 'control' information sets so that they could be sure of their validity and accuracy. For example, Linwood Service Centre staff had designed their own 'shared workspace' concept on paper and saw such a technical solution as highly desirable. However, there were significant difficulties in respect of base cost; the feasibility of cost contribution by different agencies; and in terms of the ability for other participating agencies (especially non-government) to meet the technical requirements.

NGOs have substantial technical capability problems

In several cases we could observe that non-government agencies in particular have no substantive investment in technical capability, or the means to improve that investment. A respondent from one of the refugee service agencies described the situation as follows "*we don't know what we don't know. Our hardware systems are aged. We have no funds to hire people with any technical expertise, and we cannot prioritise technical training or systems or hardware upgrades with the limited funding we do have. Unless someone was willing to provide us time and expertise on a voluntary basis we just muddle along doing what we have always done".*

Some agencies participating in information sharing initiatives are acting as 'lead' agencies with respect to information management

Because issues of information security and technical information sharing options are not well understood there was evidence that some agencies are acting as 'lead' agencies with respect to information management. In some cases, this was the agency that has greater physical, financial, or technical resources available to manage the process (e.g. Police for the POI Papakura initiative; MSD for Linwood Service Centre; Corrections for the HR/HP initiative). This enables the lead agency to control formal data sets and ensure that data are used in ways that staff interpret as most appropriate for the shared outcome sought.

Different government agencies have different interpretations of the Privacy Act, 1993, and how it should be applied

Several respondents reported an operational barrier in applying the Privacy Act, 1993, in that different government (and in some cases non-government) agencies had different interpretations of the Act and how it should be applied. When agencies are working together these different interpretations proved to be a barrier. Specific support means, such as the Information Sharing Protocol developed for the POI initiative and promulgated across all of the agencies involved with the programme, were seen as very helpful. Respondents however indicated that this is one area that would benefit from a

common interpretation and clear, unambiguous instructions regarding operational implementation.

'Vertical' information sharing practices between Head Office, local management structures and frontline operators are weaker than 'horizontal' inter-agency information sharing practices

Officials who are working for different agencies, located within the same geographical area, and involved in managing shared outcomes, have stronger working relationships with a higher level of informal and formal information sharing, compared to colleagues working for the same agency but at different levels.

For example, in one of the HR/HP case studies, front-line staff in both the Prison Service and the Community Probation Service indicated that they receive no information from the managers involved with the HR/HP forum process either about the initiative itself or about any related issues that might enable them to do their jobs better. Similarly, respondents involved in one of the POI case studies reported information gaps at both 'vertical' ends of the management process. That is, case workers were not clearly informing management about operational issues, and the governance group decisions were not being clearly represented to the front-line workers. As a consequence, people involved in the same initiative at different levels (e.g. governance and front-line operations) have different perceptions about what the initiative is trying to achieve and how it should be operated. In some cases (e.g. EM Bail) this situation meant that the management support that might have included marketing, resource allocation and management, and relationship intervention to unblock intra- and inter-agency impediments to operational practices did not occur.

However, in other case studies under the same programmes, staff from different agencies demonstrated high levels of informal and formal information sharing based on close working relationships that are characterised by trust and a clear commitment to a common outcome. In each of these cases, the management personnel effectively take personal responsibility for the success of the initiative and to a large degree either manage the operational procedures themselves (POI), or make sure that the required information is collated, and acted upon (HR/HP).

6. International Information Sharing Solutions

Introduction

In countries with similar jurisdictions to New Zealand, such as the UK, Canada and Australia, opportunities for improving cross-agency information sharing to achieve more effective social outcomes for individuals and families at risk are being explored. In so-doing solutions are being developed to overcome perceived tensions between goals of service transformation, and legal requirements to protect the privacy of individuals. In this chapter, we summarise information sharing approaches and solutions developed so far by the UK Central Government, the Canadian Federal Government and the Canadian Province of British Columbia, and the Australian Federal Government, respectively. In trying to identify opportunities for improved information sharing across agencies in the New Zealand context, a potential way forward for the NZ government could be to learn from these international approaches and arrangements.

However, in comparing our New Zealand-based research findings with existing information sharing cultures, approaches and solutions in these three overseas jurisdictions, we would like to point to the following substantially different information sharing 'realities' in other countries compared to New Zealand. First of all, information sharing approaches and strategies in overseas jurisdictions under study are usually focused on promoting (more) information sharing between agencies, whereas our research findings for New Zealand show that information sharing (already) happens, but on a 'need to know' basis. Secondly, unlike the New Zealand situation, public officials in the UK, Canada or Australia do not know each other and (therefore) do not trust each other; as a result, there is hardly any development of informal relationships between agencies, and information exchanges between agencies are completely formalised. Moreover, agencies have strong ownership perceptions of information, leading to a default position for staff to not share information. These conditions in overseas jurisdictions lead to a situation where cross-government collaboration and managing for shared outcomes is much harder compared to the New Zealand context, and privacy legislation often is perceived as a barrier to (effective) information sharing practice.

Below we describe more in detail the perspectives, approaches and information sharing solutions developed in the UK, Canada and Australia.

United Kingdom

UK Central Government

In the UK, the general legal framework for cross-government information sharing is provided by the Data Protection Act 1998, the common law, and the European Union Data Protection Directive. Moreover, the Human Rights Act 1998 safeguards the right to respect for private life, including the right to respect for personal information, under Article 8 of the European Convention on Human Rights (ECHR). In addition, especially in the last decade, a substantial number of specific legislative provisions were made under different Government Bills to enable government departments and other organisations to share data for a wide variety of purposes (e.g. the Anti-Terrorism, Crime and Security Bill, the Enterprise Bill, Community Care Bill, Criminal Justice Bill, Children Bill, Gambling Bill, Education Bill, Identity Cards Bill, Safeguarding Vulnerable Groups Bill, Welfare Reform Bill, Offender Management Bill, and the Serious Crime Bill). This overview of specific legal provisions led the UK Parliament's Joint Committee on Human Rights to the observation that "*data sharing between public sector bodies is becoming*

increasingly common… We have repeatedly expressed concerns, from a human rights standpoint, about the adequacy of the safeguards accompanying such wide powers to share personal information, but these have, for the most part, been rejected by the Government" (UK Parliament's Joint Committee on Human Rights 2008, p.8).

Others, too, signal increased ways and forms of information sharing between UK government departments, such as the growing pressure for the sharing of citizens' personal information among public service agencies as a result of the quest for more integrated forms of government (e.g. Bellamy *et al.* 2005). Crossman observes the paradigm shift in information sharing philosophy around 2002, when the Cabinet Office Performance and Innovation Unit published a consultation document 'Privacy and Data-Sharing: The Way Forward for Public Services': "*The language used was conciliatory; throughout the consultation emphasis was placed on the need to balance data sharing against privacy concerns. However, the content indicated a subtle shift in philosophy, moving away from a presumption that information should not be shared unless there is a reason to do so, towards one where information will be shared unless there is a reason to do so*." (Crossman 2007, p.175).

In 2006, a Cabinet Committee ('MISC 31') was set up to develop the UK government's strategy on data sharing across the public sector. A new high-level outline strategy for information sharing was announced in September 2006 and a comprehensive plan for data sharing promised for April 2007, but never appeared (Bellamy *et al*. 2008, p.737). Instead, in 2007, the UK Prime Minister commissioned the UK Information Commissioner Richard Thomas and Director of the Wellcome Trust Dr Mark Walport to conduct an independent review of the framework for the use of personal information in the public and private sectors. The terms of reference for this commissioned activity required the reviewers to consider whether changes are needed to the operation of the Data Protection Act 1998, to provide recommendations on the powers and sanctions available to the Information Commission and the courts in the legislation governing data sharing and data protection, and to provide recommendations on how data-sharing policy should be developed to ensure proper transparency, scrutiny and accountability.

In general, Thomas & Walport point out that it is impossible to take a generic view of data sharing: "*data sharing in and of itself is neither good nor bad. There are symmetrical risks associated with data sharing – in some circumstances it may cause harm to share data, but in other circumstances harm may be caused by a failure to share data. Data sharing needs to be examined in specific terms. Is the sharing of particular elements of personal information for a defined purpose in a precise fashion, likely to bring benefits that outweigh significantly any potential harm that might be associated with the sharing?*" (Thomas & Walport 2008, p.i).

On the basis of their consultation, Thomas & Walport come to the conclusion that "*in the vast majority of cases, the law itself does not provide a barrier to the sharing of personal data…*". However, "*the Data Protection Act is still commonly cited as a reason not to release information when it may be perfectly legitimate and in the public interest to do so…*" As a result, "*it is clear that the framework [for the use of personal information in the public and private sectors] as it stands is deeply confusing and that many practitioners who make decisions on a daily basis about whether or not to share personal information do so in a climate of considerable uncertainty*" (Thomas & Walport 2008, p.1).

Thomas & Walport make several recommendations in their report, including the following:

- the most important recommendation in their view is to establish a significant improvement in the personal and organisational culture of those who collect, manage and share personal data. Rigorous training of those responsible and accountable for the handling of personal information, backed-up by enhanced professional development, accountability, reporting and audit, will effect a major improvement in the handling and sharing of personal data;
- A strong Information Commission with sufficiently robust powers (e.g. stronger inspection and audit powers) and sanctions (e.g. financial penalties) available is needed to facilitate these cultural improvements;
- There should be a statutory duty on the Commission to provide a code of practice for the sharing of personal information to remove the 'fog of confusion' about the circumstances in which personal data may be shared;
- There should be a fast-track legislative framework that will enable transparent Parliamentary consideration as to whether any existing statutory bar to the sharing of personal information should be removed for particular purposes; and
- Research and statistical analysis for evidence-based public policy making should be enabled in a way that provides the maximum protection to the privacy of individuals.

The UK government's response to the report endorsed the reviewers' key findings and recommendations and noted that the appropriate legislative mechanism to authorise or require a data sharing arrangement needs to be decided on a case by case basis. The response also stated that the UK government is keen to counter the common misconception that the Data Protection Act is always a bar to data sharing: "*There is an appropriate balance that must be struck between the requirement to share data and the understanding that failure to share data also carries risks to vulnerable groups and individuals. The sharing of personal data between Government departments in a secure and appropriate manner is essential to protect the public and to deliver public services. The ability of Government to share data performs a crucial role in, among other things, protecting children and other vulnerable groups and individuals; it protects individuals against crime and disorder; and improves health and education provision. The ability of Government to share data between departments is essential in providing and improving customer-focused public service delivery and also ensures individuals get the services they require*." (Ministry of Justice 2008, p.5).

In several areas, such as the domain of children or identity cards, the UK Government has decided to support this required ability of information sharing between government departments and other service providers by developing large centralised databases. For example, in the area of children, a persistent theme of child abuse inquiries in the UK in the last 30 years has been deficiencies in inter-professional communication and multi-agency intervention (Peckover *et al*. 2008, p.376). As a result, under the Every Child Matters Programme, a national online directory system 'ContactPoint' with basic personal information on all children in the UK is being set up to improve cross-agency information sharing and promote early intervention. Perceived benefits of the system are helping practitioners to provide support for children who receive services across, or move across, local authority boundaries; quicker assessment of universal services being provided (e.g. education, primary health care); and more effective multi-agency working leading to less duplication of work and a better service experience for children and young people.

However, early research into the experience of professionals working with the new system in different regional areas points out that practitioners are not inclined to work with the system, and that the use of this technical solution in professional practice is highly contingent upon local policy implementation, the local arrangement of services and

the everyday practices of busy and sceptical practitioners (Peckover *et a*l. 2008). The researchers also report that the system as currently configured appears to have little in the way of panoptic potential, and that the IT infrastructure in many child welfare contexts is inadequate to ensure up-to-date records are kept (Peckover *et al*. 2008, p.391).

Furthermore, based on a recent research effort to map and assess forty-six large centralised databases used across UK government departments, Anderson et al. (2009) conclude that a quarter of the reviewed databases are almost certainly illegal under human rights or UK Data Protection law. Moreover, more than half of the reviewed databases have significant problems with privacy or effectiveness and could fall foul of a legal challenge. In summary, fewer than 15 per cent of the assessed public databases are perceived to be effective, proportionate and necessary, with a proper legal basis for any privacy intrusions (Anderson *et al.* 2009, p.4).

In general in the UK, there appear to be two seemingly opposed, emerging perspectives on the use of ICTs for cross-agency information sharing purposes, and their implications: one perspective points to the development of a 'Surveillance State', whereas another perspective focuses on the emergence of a more effective 'Service State' (Lips *et al.* 2009). As an example of the latter perspective, several UK policy developments point at the importance of technology enabled 'service transformation'. The UK Central Government Policy Strategy 'Transformational Government – Enabled by Technology' (2005) for instance presents an agenda of key public sector transformations in which information sharing will play a major role, including citizen-centric public service design and an increased uptake of shared services to release efficiencies.

A further example is a 2006 government report on Service Transformation presented by Sir David Varney, who points at the opportunity of using a cross-government IDM system for achieving effective public service transformation (Varney 2006). In presenting the now infamous Whitehall example of how a bereaved UK citizen needs to address government service counters about forty four different times, Varney makes a clear case for further examining the scope for coordinating and integrating front-line service delivery to citizens and reducing the duplication of business processes in government, through cross-government information sharing (Varney 2006). Moreover, following up Sir David Varney's report on service transformation, a current UK initiative is the 'Tell us Once' pilot project, led by the UK Department of Work and Pensions and involving a broad cross-government partnership including HM Revenue and Customs, local authorities, the Driving and Vehicle Licensing Agency and the Identity and Passport Service. As a result of this initiative, in future citizens only have to tell government once when registering a birth, death or a change of address. Current trials in place at 15 local authorities offer citizens the option to have a face-to-face interview, telephone service or web-based service, to allow them to notify government only once of a death, or to report the death to government in the normal way.

An example of the first mentioned perspective of the UK becoming a 'Surveillance State' as a result of using ICTs for improving cross-government coordination and information sharing, is a June 2008 Speech on Security and Liberty by the UK Prime Minister, in which he emphasised the need to preserve individual liberties when introducing new ICT-enabled measures to fight crime and terrorism, such as those relating to identity cards, the National DNA Database, and CCTV. Furthermore, in May 2008, the House of Commons' Home Affairs Committee called on the UK Government to give proper consideration to the risks associated with increasing and excessive ICT-enabled 'surveillance', i.e. the collection and processing of citizens' personal data, as the resulting loss of privacy erodes trust between the individual and the Government and can change the nature of the relationship between citizen and state (House of Commons 2008).

More recently, in 2009, based on an inquiry into the impact that government surveillance has upon the privacy of citizens and their relationship with the state, the House of Lords' Select Committee on the Constitution similarly concluded that there has been a profound and continuous expansion in the surveillance apparatus of the state (House of Lords 2009). Examples mentioned were the growing use of CCTV cameras in public places, increased reliance on the interception of communications by the police and security services, and a national scheme of identity cards. In the view of the House of Lords' Select Committee, to respond to crime, combat the threat of terrorism, and improve administrative efficiency, the development of ICT-enabled surveillance and the collection and processing of personal information have become pervasive, routine and almost taken for granted in British society, with data being collected on the entire population and not just on traditional "suspects" (House of Lords 2009).

The House of Lords' Select Committee on the Constitution did acknowledge that the processing of personal data has always been part of public administration, and that it is essential to effective governance and efficient service delivery. However, they perceived a distinction of contemporary uses of surveillance and data processing from those of the past in the extent and intensity with which information is analysed, collated, and used. Regarding privacy and the principle of restraint in the use of surveillance and data collection powers as central to individual freedom, the Select Committee observed a serious threat to these principles as a result of the growing use of surveillance by government (House of Lords 2009, p.9-10). Recommendations made by the House of Lords' Select Committee on the Constitution included the adoption of a principle of data minimisation by government departments; broadening and strengthening the powers of the UK Information Commissioner; enhanced information security; citizen-centred IDM solutions; and training and raising awareness about the legal meanings of necessity and proportionality in the collection and processing of citizens' personal information.

During the time that the UK government sought to further increase ICT-enabled cross-agency information sharing, the UK public sector experienced a number of high-profile 'Data Loss Incidents' (DLIs). Since 2007, DLIs include the loss or theft of a substantial number of memory sticks across government and private sector (sub-)contractors of government, with several sticks holding sensitive data, such as medical information of more than 6,000 prisoners and ex-prisoners; information on all 84,000 prisoners in England and Wales; and personal details of about 10,000 prolific offenders; DLIs also involve the loss or theft of computer and portable hard drives containing for instance personal details of about 600,000 people who had expressed an interest in the Royal Navy, Royal Marines and the RAF (including bank details and National Insurance numbers); personal details of about 3 million candidates for the UK driving theory test in the USA; and the loss of computer discs containing personal details of about 25 million child benefit recipients (including bank details and National Insurance Numbers). These DLIs have contributed to a public perception of "institutionalised incompetence" of government agencies to appropriately manage (sensitive) personal data on the citizen (BBC News 2008).

Canada

Canadian Federal Government

There is no federal government strategy dedicated to cross-government information sharing in Canada. Moreover, there is no specific provision in the Canadian Federal Privacy Act 1982 relating to data sharing. However, section 8 (2)(m) of the Canadian Privacy Act 1982 permits government institutions to disclose personal information, without the consent of the individual concerned, for any purpose where, in the opinion of the head of the institution, the public interest in disclosure clearly outweighs any invasion

of privacy that could result from the disclosure, or disclosure would clearly benefit the individual to whom the information relates.

From a cross-government information sharing perspective, the Canadian legislative framework currently has four general restrictions with regard to the collection, use and disclosure of personal information between agencies (Trudel *et al*. 2007, p.2). Firstly, under current Canadian privacy legislation, the collection of personal information would involve a government agency requiring or requesting individuals to identify themselves via the use of an identifier. In order for the agency to "collect" the identifier, it must either be previously authorized by a statute to collect the personal information concerned or the collection must be reasonably necessary for the carrying out of a lawful activity performed by that agency. A second restriction with regard to the collection of personal information is that the information should be direct, i.e. obtained from the person to whom the information relates. Thirdly, the use of personal information is restricted to the purpose for which that information has been collected. And fourthly, a public body may not, as a general rule, communicate personal information that is in its possession to a third party. However, the release of personal information is permitted if expressly authorized by law. This exchange of information may be formalized in an information sharing agreement.

In general, solutions for improving cross-government information sharing appear to be sought in the establishment of Memorandums of Understanding (MoUs) and information sharing protocols between agencies concerned. Clear rules regarding information sharing between various jurisdictions are expected to promote cross-government information sharing, improve the coordination between various levels of government, and increase transparency (Lacroix et al. 2004). Furthermore, in areas of individuals and families at risk, several provincial governments in Canada have identified the need for greater cross-government coordination and information sharing and put information sharing protocols in place (e.g. Novia Scotia's 'High Risk Case Coordination Protocol Framework. Spousal/Intimate Partner Violence', Manitoba's Information Sharing Protocol under the Youth Criminal Justice Act).

Province of British Columbia

In British Columbia, there has been significant pressure in recent years to increase the amount of data sharing between government agencies. Traditionally, government programme implementation and service delivery has been the responsibility of each individual agency. It is acknowledged that a cohesive flow of information between agencies can reduce the duplication of services, and limit inappropriate intervention or lack of action when action is necessary. For example, in the Canadian health sector, there is crossover between the Federal government (Health Infoway), the Ministry of Health (Medical Service Plan, Master Patient Index), Health Authorities, community intervention projects, private labs and private physicians (Office of the Government CIO 2008, p.2).

Improved information sharing therefore requires coordination and collaboration between multiple levels of government and the private sector, and would bring about the delivery of timely and effective services to the public, streamline service provision and achieve the goal of better outcomes for citizens. Available technology has been acknowledged as an enabler for establishing this new model of 'Citizen Centered services' and, with that, as an important means to communicate for the purposes of information sharing.

In British Columbia, the Office of the Government Chief Information Officer is responsible for provincial legislation in the domain of privacy and the protection of personal information. While acknowledging increasing privacy-related risks in widening

the basis for the sharing of personal information, the provincial government is developing initiatives to improve public service delivery and efficiencies through more widespread disclosure of citizens' personal information across agencies. The Office of the Information and Privacy Commissioner for British Columbia is actively monitoring and providing comment to these initiatives to ensure that they comply with the existing privacy law and meet reasonable privacy expectations (OIPC for BC 2009, p.8).

One of the initiatives taken in British Columbia is the development of a provincial identity management (IDM) framework. This initiative aims to meet the need to share information in three particular ways (Watkins 2007 p.3):

1. **Information sharing for research purposes**. British Columbia recognises that solutions to its most complex social issues will not be found within one organisation or sector. Education, for example, has profound impacts on health and social welfare. Researchers and policy makers must therefore have access to information across sectors both to develop and evaluate public policy.

2. **Information sharing for frontline service providers**, in particular the need to share information across health, social, education and criminal/justice sectors. Homeless citizens, as an example, frequently face a myriad of concerns beyond a lack of housing (e.g. addictions, mental and physical health challenges, unemployment, and poverty). What is becoming increasingly clear is that an uncoordinated approach across sectors makes the task of improving citizen outcomes extremely difficult.

3. **Information sharing for citizen self-service.** In British Columbia, citizens are increasingly using online services to conduct business and organise their lives. To establish a truly citizen-centric government, the Province of British Columbia needs to establish IDM and security protections that will enable greater online service.

The challenge perceived here is being able to coordinate activity and share information appropriately across agencies. Reorganisation so as to consolidate organisations that must work together to improve outcomes, was not perceived as a suitable answer, as any given organisation contributes to outcomes from widely spaced public service domains. Moreover, consolidation in order to establish political and management authority within a single organisational context with the aim to overcome barriers to information sharing, could lead to an unacceptable consolidation of power. As a result, the solution has been to develop an IDM system which supports cross-government information sharing and enhances privacy protection at the same time. The developed IDM solution includes a claims-based, user-centric architecture.

As indicated earlier, in Canada, an important barrier to improving information sharing across agencies is perceived to be in current legislation in the area of personal information protection. For instance, in British Columbia, the following lessons were learned from a policy analysis of legal barriers and enablers of information sharing across government, based on a comparative analysis of the three provincial Acts regulating the collection, use and disclosure of personal information by, and between parties (i.e. FOIPPA, PIPA and PIPEDA) (Office of the Government CIO 2008, p.10):

- Information sharing is limited, but not impossible. The three Acts set out very specific circumstances when personal information may be collected, used and disclosed. Health care, legal matters, law enforcement, and debt collection are common themes across the Acts through which certain information sharing options are available.
- The ability to share information depends upon who is sharing the information, and how. The ability to collect and/or disclose information between two or more

- Private organizations have much more stringent provisions protecting the collection, use and disclosure of personal information. PIPA and PIPEDA are based on consent. They are more restrictive with respect to the collection, use and disclosure of personal information without consent. FOIPPA provides more flexibility comparatively with respect to the disclosure of personal information.
- PIPEDA limits personal information flow more than PIPA. PIPA includes a provision that allows for implicit consent, providing increased flexibility over PIPEDA with respect to information sharing in certain circumstances.

Furthermore, officials from British Columbia acknowledge that implementing complex information sharing agreements across several parties is difficult, especially when the parties are located in both the private and public sectors. This complexity often requires that needs for information sharing are examined on a case by case basis.

Australia

The Australian Federal Government

The Australian Federal Privacy Act, 1988, does not contain a specific provision for information sharing between public sector agencies. In general, the Information Privacy Principles, and exceptions to these principles, determine whether or not agencies can share information. Furthermore, the Act empowers the Federal Privacy Commissioner to make Public Interest Determinations (PIDs). A PID is a determination on the basis of public interest that an act or practice of an agency, which would otherwise breach an Information Privacy Principle or an existing privacy code, is to be regarded as not breaching the principle or code concerned.

Commissioned by the Council of Australian Government's (COAG) Online and Communication Council in July 2007, the Australian Federal Government recently adopted a National Government Information Sharing Strategy (NGISS). Aim of the NGISS is to provide (Commonwealth of Australia 2008a, p.5): "*a standardised approach to information sharing to support the delivery of government services to the Australian community. The expectation is that the national strategy can be used by all portfolio areas at all levels of government".* Research conducted for the development of the NGISS identified the following structural barriers to successful information sharing across agencies (Commonwealth of Australia 2008a, p.10-11):

1. **Leadership at political and senior executive levels:** competing agenda and differing goals across, and within, the three tiers of government make it difficult to gain cohesive support for information sharing from public sector leaders. In many cases, executives focus on protecting agency information as a priority and are not aware of the benefits of sharing this information with other agencies and levels of government where it is legitimate to do so.
2. **The absence of clear value proposition:** the usefulness of information gathered by one agency to another part of the same agency, or other agencies or jurisdictions, is not recognised; excessive cost-recovery policies can inhibit re-use of information; or information and its associated intellectual property is undervalued and shared too freely.
3. **The absence of a common approach to information management practices**: this leads to difficulties in several areas of information sharing, such as the

4. **Complex privacy legislation and related accountability issues**: The complexity of Australian privacy laws which, according to the Australian Law Reform Commission, are multi-layered, fragmented and inconsistent, often results in the default response to requests for information (that might be considered sensitive) as: "*We cannot share our information because of privacy laws*." This response is often given instead of determining (through the appropriate channels) whether the information can, in fact, be shared.
5. **Non-Sharing Culture**: research findings demonstrate that there is still a culture of '*information is power*' that results in the defensive protection of an organisation's information assets. Added to this is the fact that knowledge management practices are poorly defined and applied. There is also a generational divide in terms of attitudes towards information sharing. Younger generations have grown up in a world where the information they need is readily available and easily shared, whereas, older generations have generally not experienced or adopted such sharing approaches.

The following NGISS Information Sharing Principles were identified as essential for successful information sharing:

- Provide leadership;
- Demonstrate value: move from 'need to know' to 'need to share';
- Act collaboratively;
- Establish clear governance;
- Establish custodianship guidelines;
- Build for interoperability;
- Use standards-based information;
- Promote information re-use;
- Ensure privacy and security

The NGISS is to be followed by an implementation plan to identify and report on progress across all jurisdictions. Implementation strategies are grouped under four areas: awareness raising; improving governance; management and planning; and enabling tools.

Similar research findings to those from the NGISS development study mentioned above can be found in specific domains focused at individuals and families at risk. An example is a recent study conducted to assess what the Australian federal government can do to improve the effectiveness of information sharing for families and children in the child protection system (Commonwealth of Australia 2008b). In general, the research findings demonstrate that information sharing can and does occur under current legislation. However, there is a low level of understanding of what information can be requested and how to manage information requests.

The following key barriers to effective information sharing were identified:

- **Provisions in legislation for the sharing of information:** while there are legal avenues available for information sharing, requesting agencies report that legal obligations are often given as a reason why information cannot be disclosed;
- **The lack of agreed processes:** child protection agencies are not typically aware of what sort of information other agencies hold; there is no national standard process for requesting information; and there are inconsistent views around the application of legal thresholds;

- **Risk aversion in organisations:** stakeholders report risk aversion on the part of both requesting and responding, likely as a result of the two barriers above

The following suggestions for improvements were made, without undertaking legislative change:

- Facilitating and expanding the Commonwealth's role in information sharing: agree a protocol for information sharing between agencies concerned so to establish clear processes for information sharing;
- Improve understanding and consistent application of legal thresholds for information disclosure: as part of developing the information sharing protocol, Centrelink should review its guidelines for information sharing and organise the training of staff to ensure there is a good understanding and consistent implementation of guidelines
- Include Centrelink in the interstate alerts system;
- Consider the appropriateness of thresholds for disclosure in review of secrecy provisions; and
- Explore further opportunities for information sharing with other parties, including Medicare Australia, Family Court, Department of Immigration and Citizenship.

7 Improving information sharing for effective social outcomes: solutions and recommendations

Introduction

Based on the case study findings, the review of international information sharing solutions, the discussion of the case study findings in focus group meetings and feedback sessions, and solutions suggested in the focus group meetings and feedback sessions, the following solutions and recommendations for improving cross-government information sharing in the New Zealand context have been developed. With that, we provide an answer to the research question of how, and under what conditions, cross-government information sharing can be improved in order to achieve more effective social outcomes.

Solutions and recommendations for improving information sharing

The empirical findings from this research show that officials are conscious about the need to protect the personal information of clients and are acting upon this need: for instance, they share information on a 'need to know' basis, and use signed consent forms as authorisation to share information with other agencies. Privacy values are embedded in the way that officials work and, with that, these values shape operational information sharing practice. Furthermore, in situations where there are professional, personal and/or community safety risks related to the confidentiality of personal information on the client, staff members of agencies operating under a public safety mandate can rely on Principle 11 of the Privacy Act, 1993, to share critical information with other professionals. Generally therefore, and in line with operational practice, existing privacy legislation appears to offer an appropriate 'default position' for government agencies to share information, and to provide enough room for information sharing arrangements.

However, we observed clear differences in information sharing procedure and practice between agencies operating under a public safety mandate, and agencies with a public service mandate. Although agencies operating under a public service mandate experience similar safety risks related to the confidentiality of an individual's personal data compared to agencies operating under a public safety mandate, public service organisations do not have a legal 'back-up' when they share critical information with other professionals. Moreover, not having a legal provision for sharing critical information on individuals at risk, leads to ambiguous situations around legal boundaries of information sharing in dealing with other agencies (public service providers, agencies with a public safety mandate, and community service providers). As a result, professionals experience uncertainty about whether, and if so what information can be shared, and therefore often decide not to share critical information.

This default position of not sharing information leads to situations in which the complex needs of the client are not being met; professionals being exposed to danger without their knowledge; and clients at risk needing to join-up agencies themselves in order to consume the required integrated services. This default position also stands in the way of sharing information with public service providers in the health domain and/or with health practitioners, which is often required to do a professional job towards individuals or families at risk.

For these reasons we conclude that there is a clear need for legal support of information sharing in the area of providing social services, similar to the working of Principle 11 under the Privacy Act, 1993. A legal precedent for sharing critical information under

privacy legislation in line with Principle 11 under the New Zealand Privacy Act, 1993, can be found in the Information Privacy Bill, 2007, of Western Australia, where the following legal provision exists: a "*disclosure to lessen or prevent a serious threat to an individual's or public welfare*".

Solution 1: ***Under the current privacy legislation, create a Code of Practice for Welfare***

As information sharing is strongly related to trust in relationships with other professionals, and information sharing protocols focused on a clear commitment to a shared outcome are useful for developing relationships with other agencies, building trust amongst professionals, and providing clarity about the application of legal provisions, we propose to use information sharing protocols to improve information sharing across agencies. A good example of an information sharing protocol developed in conjunction with the Office of the Privacy Commissioner is the information sharing protocol used under the Priority Offenders Initiative. Besides a regular evaluation of the functioning of an information sharing protocol by Head Office, a local team evaluation could help identifying practical barriers to information sharing at an early stage (e.g. high case volumes; particular agencies needed at the table; personality problems within the team).

Solution 2: ***Use Information Sharing Protocols focused on a clear commitment to a shared outcome to build professional trust and relationships across agencies***

Recommendation 1: ***Organise a local team evaluation of the functioning of the information sharing protocol arrangement on a regular basis***

We observed that professionals are most exposed in obtaining critical medical information on individual clients, and that health information is the area in which safety issues are most likely to arise. Moreover, not sharing health-related information between professionals can compromise clients from receiving services they are entitled to. However, professionals usually are not inclined to share health-related information.

Solution 3: ***In designing Information Sharing Protocols, pay special attention to the interface with health information***

We propose that NGOs be included in future information sharing protocols to overcome current 'grey areas' around information sharing procedure and practice between government agencies and community-based service providers.

Solution 4: ***Include NGOs in information sharing protocols***

We observed the importance of trust as a precondition for effective information sharing and concluded that the quality of information sharing depends on the quality of relationships between individual professionals. Moreover, where there is a culture of working together for shared outcomes there is more co-operation and less ambiguity about information sharing. Based on these research findings we conclude the critical importance

for an agency to select a representative with the right relationship and trust building qualities for participation in a cross-government initiative, in order to enable effective information sharing. Consequently, agencies will need to look for candidates with the right qualities for successful cross-government collaboration. In earlier research, we made some specific recommendations in that respect (see the research findings of the EIP JUG project).

Solution 5: Selection of the right agency representative for participation in a cross-government initiative is critical for enabling effective information sharing

With the observation that the quality of information sharing depends on the quality of relationships between individual professionals, the facilitating role of the Chair person in cross-government initiatives becomes of importance. In order to bring the right set of agencies to the table (in terms of both sector representation and volumes), to facilitate agreement between professionals on the shared outcome of information sharing, and to enable the development of relationships and trust between professionals, agencies also will need to look for suitable candidates who can effectively act as the *primus inter pares* and provide facilitative leadership to the group of professionals. Facilitative leadership could further include acting as the 'lead' agency with respect to information management, such as dealing with issues around ownership of shared information or providing technical support for managing the process (e.g. offering access to a secure shared workspace).

Solution 6: Arrange for facilitative leadership in a (horizontal) information sharing arrangement

Co-location of organisations (government and non-government) that provide services to the same target group of individuals and families with complex needs enhances opportunities to develop relationships with other agencies, build trust among professionals and, with that, support information sharing practice. However, issues around the management of shared records and ownership of information (e.g. which agency deals with an OIA request?) need to be taken into account when exploring or implementing a co-location solution.

Solution 7: Explore co-location opportunities for service providing partner organisations

In several cases (e.g. HR/HP forums), more routine information sharing practices lead to rapidly increasing case volumes. This situation can get unmanageable and will require a redesign of the information sharing process. For example, in the case of HR/HP, the current information sharing process could be split up in an eight months preparation meeting of frontline operators and a four months meeting in which senior management signs off cases.

Solution 8: When information sharing is routine and case volumes are rapidly increasing the information sharing process needs to be subject to reconsideration

Officials constantly make judgments about the validity of information, whether they can use that information officially or if they can act on it unofficially, and what information can be shared with whom and for what purpose. Although public sector staff receive regular training on the application of the Privacy Act, 1993, they often lack information on the ways and extent to which they can share information on the client with other professionals. NGOs usually do not have the financial resources to offer their staff training related to the Privacy Act. In addition, an area which has not been further explored by most agencies so far (a good exception is the Priority Offenders Initiative), is the systematic application of de-personalised ways of information sharing on the client. These alternative ways of information sharing support an individual's privacy protection and enhance information security.

Solution 9: ***Provide training and education on the do's and don'ts of information sharing under privacy legislation, across the public sector and NGOs***

Recommendation 2: ***Lower the fees for privacy legislation training and education to NGOs***

Recommendation 3: ***Further explore de-personalised ways of sharing information***

Frontline staff members involved in horizontal information sharing initiatives experience a lack of clarity about the correct interpretation of the Privacy Act, 1993, due to the fact that different government agencies have different interpretations of the Act, and how it should be applied.

Solution 10: ***Head offices of agencies involved in an information sharing arrangement need to provide explicit, joint guidance on (the implementation of) a uniform interpretation of the Privacy Act, 1993***

Vertical information sharing practices between Head Office, local management structures and frontline operators demonstrate weaknesses, such as information gaps and different perceptions about what the initiative is trying to achieve, which could be managed.

Solution 11: ***There needs to be more attention for increasing the effectiveness of vertical information sharing between Head Office, local management and front-line operators, including an understanding of different information needs at the various levels***

In many cases, technical solutions for improved information sharing are available, but unused. Furthermore, NGOs have no substantive investment in technical capability, or the means to improve that investment. By making use of available technical solutions and investing in technical capability as well as technical literacy, across the public sector and

NGOs, information security and the protection of personal information in cross-agency information sharing initiatives can be improved substantially.

Solution 12**:* ***Provide representatives of participating government agencies and NGOs with access rights to a secure information system.

Solution 13: ***Use shared secure workspaces across information sharing collaborators including NGOs***

Solution 14: ***Further invest in technical capability as well as technical literacy, across the public sector and NGOs***

Academic references

6, P. (2004). Joined-up government in the western world in comparative perspective: A preliminary literature review and exploration. *Journal of Public Administration Research and Theory, 14*(1), 103–138.

6, P., Goodwin, N., Peck, E., & Freeman, T. (2006). *Managing networks of twenty-first century organisations*. Basingstoke, Hampshire UK, New York: Palgrave Macmillan.

6, P., Raab C.D. & Bellamy, C. (2005). Joined-up government and privacy in the UK part I: managing tensions between data protection and social policy. Part I. *Public Administration* 83(1), 111–133.

Agranoff, R., & McGuire, M. (1999). Managing in network settings. *Policy Studies Review, 16*(1), 18–41.

Agranoff, R., & McGuire, M. (2001). Big questions in public network management research. *Journal of Public Administration Research and Theory, 11*(3), 295–326.

Anderson, R., I. Brown, T. Dowty, P. Inglesant, W. Heath & A. Sasse (2009). *Database State*, March 2009, a report commissioned by the Joseph Rowntree Reform Trust Ltd., The Joseph Rowntree Reform Trust Ltd., York.

Bellamy, C., 6, P., Raab, C.D., Warren, A., & Heeney, C. (2008). Information sharing and confidentiality in social policy: Regulating multi-agency working. *Public Administration, 86*(3), 737–759.

Bellamy, C., Raab, C.D., Warren, A., & Heeney, C. (2007). Institutional shaping of interagency working: Managing tensions between collaborative working and client confidentiality. *Journal of Public Administration Research and Theory, 17*(3), 405–435.

Bellamy, C., Raab, C.D., and 6, P. (2005). Multi-agency working in British social policy: Risk, information sharing and privacy. *Information Polity*, 10 (1-2), 51-63.

Bertot, J.C. and Jaeger, P.T. (2008). The E-Government paradox: Better customer service doesn't necessarily cost less. *Government Information Quarterly*, 25 (2) 149-154

Bryson, J. M., Crosby, B. C., & Middleton Stone, M. (2006). The design and implementation of cross-sector collaborations: Propositions from the literature. *Public Administration Review*(Special Issue), 44–55.

Conklin, E. J. (2006). *Dialogue mapping. Building shared understanding of wicked problems*. England: John Wiley and Sons.

Crosby, B., & Bryson, J. M. (2005). A leadership framework for cross-sector collaboration. *Public Management Review, 7*(2), 177–201.

Crossman, G. (2007). The ID Problem. In: D.G.W. Birch (ed.) *Digital Identity Management. Perspectives on the Technological, Business and Social Implications*, Aldershot: Gower, pp.175-182.

Das, T. K., & Teng, B. (2001). Trust, control and risk in strategic alliances: An integrated framework. *Organization Studies, 22*(2), 251-283.

Davies, J. S. (2009). The limits of joined-up government: Towards a political analysis. *Public Administration, 87*(1), 80–96.

Dyer, J., & Chu, W. (2003). The role of trustworthiness in reducing transaction costs and improving performance: Empirical evidence from the United States, Japan and Korea. *Organization Science, 14*(1), 57-68.

Edelenbos, J., & Klijn, E.-H. (2007). Trust in complex decision making networks: A theoretical and empirical exploration. *Administration and Society, 39*(1), 25-50.

Eppel, E. (2007). *Better connected services for Kiwis: Achieving outcomes by joining up. A literature review*. Wellington: Victoria University of Wellington.

Eppel, E., Gill, D., Lips, M., & Ryan, B. (2008). *Better connected services for Kiwis: A discussion document for managers and front line staff on better joining up the horizontal and the vertical*. Wellington: Institute of Policy Studies, School of Government, Victoria University of Wellington.

Gellman, R. (2004). Privacy and security: Assessing database derivative activities. *Government Information Quarterly*, 21 (4), 498-504

Gil-Garcia, J.R., Chun, S.A., and Janssen, M. (2009). Government information sharing and integration: Combining the social and the technical. *Information Polity*, 14 (1-2), 1-10

Heen, H. (2009). 'One Size Does Not Fit All' :Variations in local networks and their management. *Public Management Review, 11*(2).

Hudson, B. (2004). Analysing network partnerships: Benson re-visited. *Public Management Review, 6*(1), 75–94.

Huxham, C., & Vangen, S. (2000). Leadership in the shaping and implementation of collaboration agendas: How things happen in a (not quite) joined-up world. *Academy of Management Journal, 43*(6), 1159–1175.

Kickert, W. J., Klijn, E.-H., & Koppenjan, J. F. M. (1997). Introduction: A management perspective on policy networks. In W. J. Kickert, E.-H. Klijn & J. F. M. Koppenjan (Eds.), *Managing complex networks: Strategies for the public sector* (pp. 1–13). London, Thousand Oaks, New Delhi: Sage Publications.

Klijn, E.-H. (1997). Policy networks: An overview. In W. J. Kickert, E.-H. Klijn & J. F. M. Koppenjan (Eds), *Managaing complex networks: Strategies for the public sector* (pp. 14–34). London, Thousand Oaks, New Delhi: Sage Publications.

Kurtz, C. F., & Snowden, D. J. (2003). The new dynamics of strategy: Sense-making in a complex and complicated world. *IBM Systems Journal, 42*(3), 462–483.

Lacroix, M., Deschenes, M., Grégoire, G., Sénécal, K., Avard, D. & Knoppers, B.M. (2004). *The Reporting and Management of Personal Information and Personal Health Information to Control and Combat Infectious Disease: An Analysis of the Canadian Statutory and Regulatory Framework*, Paper submitted to Health Canada, Centre for Surveillance Coordination, Population and Public Health Branch, March 2004, Université de Montréal

Lips, A. M.B., Taylor, J.A., & Organ, J. (2009). Managing Citizen Identity Information in E-Government Service Relationships in the UK: The Emergence of a Surveillance State or a Service State? *Public Management Review*, 11(6), pp.833-856

Mandell, M. P. (1999). The impact of collaborative efforts: Changing the face of public policy through networks and network structures. [Symposium]. *Policy Studies Review, 16*(1), 4–17.

Martin, G. P., Currie, G., & Finn, R. (2008). Leadership, service reform, and public service networks: The case of cancer-genetic pilots in the English NHS. *Journal of Public Administration Research and Theory, 19*, 769–794.

Moore, M. H. (1995). *Creating public value: Strategic management in government*. Cambridge MA: Harvard University Press.

Muthusamy, S. K., & White, M. K. (2005). Learning and knowledge transfer in strategic alliances: A social exchange view. *Organization Studies, 26*(3), 415-441.

Peckover, S., White, S., & Hall, C. (2008). Making and Managing Electronic Children: E-assessment in child welfare. *Information, Communication & Society*, 11:3, pp.375-394.

Regan, P.M. (2004). Old issues, new context: Privacy, information collection, and homeland security. *Government Information Quarterly*, 21 (4), 481 - 497

Ring, P. S., & Van der Ven, A. H. (1992). Structuring co-operative relations between organizations. *Strategic Management Journal, 13*, 483-498.

Ring, P. S., & Van der Ven, A. H. (1994). Development processes of interorganisational relationships. *Academy of Management Review, 19*(1), 90̃118.

Ritter, H. W. J., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Public Sciences, 4*, 155-169.

Roberts, A. (2004) ORCON Creep: Information sharing and the threat to government accountability. Government Information Quarterly, 21 (3), 249-267

Rommel, J., & Christiaens, J. (2009). Steering from ministers and departments: Coping strategies of agencies in Flanders. *Public Management Review, 11*(1), 79–100.

Ryan, B., Gill, D., Eppel, E., & Lips, M. (2008). Managing for joint outcomes: Connecting up the horizontal and the vertical. *Policy Quarterly, 4*(3), 14-21.

Weick, K. E. (2001). *Making sense of the organization*. Malden MA: Blackwell Publishing.

Wetmore, J.M. (2007). Distributing Risks and Responsibilities: Flood Hazard Mitigation in New Orleans. *Social Studies of Science*, 37 (1), 119–126

Further documentation used

Multicultural Service Centre for Refugees
Wellington Regional Action Plan for Refugee Health and Well-being
Cunningham, Ruth (2007) *'Dreaming a Bit': An evaluation of the Wellington Regional Refugee Health and Well-being Action Plan*, Public Health Registrar, Regional Public Health, (June).
Refugee Services Aotearoa New Zealand, *Annual Report 2007 -08*
Refugee Services Aotearoa New Zealand, *A Place to Call Home: Refugee Services Magazine,* Issue 1, March 2009
Summary of Inter Sectoral Dialogue, A record of the process and the outcome of dialogue gathered on behalf of the Inter-sectoral Working Group for the Wellington Regional Refugee Health and Well-being Action Plan

Linwood Service Centre
CD on Integrated Case Management initiative in Papakura.
Linwood Community Link – an explanation of why the centre was set up and how it works.
Model office concept @MSD – a functional view of the model office concept IT blueprint.
Linwood Community Link Client Assessment form.
Linwood Community Link consent form for sharing information.
Linwood Model Office Tool: Screening Questions
Linwood Community Link Workflow model.

High Risk/ High Profile Forums
Department of Corrections Notification of Change to Operational Policy (Circular), 25 August 2008.
High Risk High Profile Forum Guidelines

Priority Offenders Initiative
Purpose Specific Information Sharing Protocol, CSPIN Top Ten Family Strategy, August 2006
Walker, Ann Sarah (2007), *The Strengthening Families Strategy: An enduring model of interagency collaboration in an era of change,* Victoria University of Wellington, Chapter 7.
Priority Offenders Initiative Practice Guide, Ministry of Justice and NZ Police, 2008.

Electronic Monitored Bail
EMBP-20 Request for Information – CYF
EMBP-09 Request for Information – CPPS
EMBP-10 Request for Information – Health Provider
EMBP-08 Request for Information – Prison/ Residence
EMBP-07 Request for Information – Court
EMBP-21 Request for Information – Housing NZC
Application for bail with electronic monitoring
Electronic Monitoring on Bail, FAQ, http://www.police.govt.nz/service/embail/faq.html
Electronic Monitoring on Bail http://ww.police.govt.nz/service/embail/
Developments in EM bail, New Zealand Law Society, 2008
Interim Policy on Bail with Electronic Monitoring, Legal Services Agency
Beaumont, Nathan and Burgess, Dave *Review of electronic bail after breaches,* Dominion Post, 7 March, 2009.

Additional materials

BBC News, *Discs loss 'entirely avoidable*', 25 June 2008, available at:
http://news.bbc.co.uk/2/hi/7472814.stm

Commonwealth of Australia (2008a). *National Government Information Sharing Strategy*, Australian Government Information Management Office, available at: http://www.finance.gov.au/publications/national-government-information-sharing-strategy/docs/ngiss.pdf

Commonwealth of Australia (2008b) I*nformation sharing to assist families and children in the child protection system. What the Commonwealth government can do*, September 2008, Report to the Australian Government's Department of Families, Housing, Community Services and indigenous Affairs by The Allen Consulting Group, available at: http://www.fahcsia.gov.au/sa/families/pubs/Documents/information_sharing/default.htm

House of Commons Home Affairs Committee (2008) *A Surveillance Society?*, Volume 1, Fifth Report of the Session 2007-08, 20 May 2008, London: The Stationery Office.

House of Lords Select Committee on the Constitution (2009) *Surveillance: Citizens and the State. Volume 1: report*, 6 February 2009, 2nd Report of Session 2008-09, London: The Stationery Office

Ministry of Justice (2008). *Response to the Data Sharing Review Report*, 24 November 2008, Available at: http://www.justice.gov.uk/publications/response-data-sharing-review.htm

Office of the Government Chief Information Officer (2007) *Information Sharing Across Government: An Analysis of Legislative Barriers and Enhancers,* British Columbia, IM/IT Privacy and Legislation Branch.

Office of the Information & Privacy Commissioner for British Columbia (2009). Office of the Information & Privacy Commissioner for British Columbia's Annual Report 2008–2009. Available at: http://www.oipc.bc.ca/publications/annual_reports/OIPC_AR_2008_09.pdf

PM's Speech on Security and Liberty, 17 June 2008. Available at http://www.number10.gov.uk/Page15785

Thomas, Richard & Walport, Mark (2008). *Data Sharing Review Report*, 11 July 2008

Trudel, Pierre, Brabant, Katerine and Arless-Frandsen, Ruth (2007) *Review of Federal and Provincial Statutes Governing Individual Identification Information and Interjurisdictional Exchange of Personal Information,* University of Montreal.

UK Parliament's Joint Committee on Human Rights, 14th report of 2007/2008, available at: http://www.publications.parliament.uk/pa/jt200708/jtselect/jtrights/72/72.pdf

Varney, D. (2006). *Service Transformation: A better service for citizens and businesses, a better deal for the taxpayer*, London, HMSO, available at: http://www.hm-treasury.gov.uk/media/4/F/pbr06_varney_review.pdf

Watkins, Peter (2007). Trust and Identity Management. Experience and perspective from the Province of British Columbia, Canada, paper presented at the Trust Conference e-Government Identity Management Initiatives, 21–22 November 2007, The Hague.

Appendix 1: Assessment of case studies against selection criteria.

(1) Multicultural Service Centre for Refugees

With respect to the selection criteria for the study, the organisations work with vulnerable individuals and families dealing with complex problems at the intersection of multiple policy domains (e.g. social, economic and justice; social, education and health). They collectively provide a range of services to the same group of people, but are not necessarily privy to the information provided to the others, depending on its nature.

Services to refugees are provided by a range of government and non-government organisations and therefore multi-agency co-ordination and co-operation is critical to maintaining service quality. A collective, inter-sector action plan was developed in 2005/6 with different agencies taking a lead role in addressing key issues. The following table summarises the match between the criteria for selection and this case study:

Programme	Indiv/ FAR	Complex Problems	Govt/Non-govt	Ethnic var	Vol/Comp	Information Sensitivity	Tech
Multicul-tural Service Centre	Indivs and families at risk	Housing; Health; Education; Employ-ment; Language; Mental Health; Resettle-ment needs	Non-Govt	People from a wide variety of nations	Voluntary participation by clients	Personal; Health; Family matters	Low

(2) Linwood Service Centre

The Linwood Service Centre delivers services to individuals seeking income, housing, employment and other types of welfare assistance. Their needs are often complex and relate to a variety of policy domains (e.g. social, economic and justice; social, education and health). The agencies participating in the Service Centre provide a range of services based on entitlement and advocacy. Some sets of information on individuals are shared, depending on the service being provided.

The following table summarises the match between the criteria for selection and this case study:

Prog	Indiv/ FAR	Complex Problems	Govt/Non govt	Ethnic va	Vol/Comp	Information Sensitivity	Tech
Integrated Service Response (Linwood Service Centre, Christchurch)	Indivs	Income support; Employment; Housing; Welfare.	Mix	Pan-ethnic	Vol	Personal; Health; Family matters	Med

(3) High Risk/ High Profile Forums

The HR/HP forums offer an alternative model of information sharing. Individuals discussed in this forum are unaware it operates and have no choice in the process. It is a management process designed to maximise communication between various parties responsible and accountable for the effective management of a common set of individuals. The needs of the individuals are often complex and require co-ordination across diverse interests. Community safety and security can be affected negatively when communications and co-ordination are not managed appropriately.

This initiative is primarily an internal communications alignment process. External agencies (Police) are involved on the basis of ensuring community safety is enhanced. Other external agencies are involved in managing release arrangements (e.g. housing, treatment facilities) but are not included in the forum.

The following table summarises the match between the research criteria for selection and this case study:

Prog	Indiv/ FAR	Complex Problems	Govt/Non-govt	Ethnic var	Vol/Comp	Information Sensitivity	Tech
HR/HP	**Indivs**	**Offending history; income; employment; housing; mental health; complex family interactions.**	**Govt**	**Pan-ethnic**	**Comp**	**Personal; Health; Mental health; Family matters; offending history**	**High**

(4) Priority Offenders Initiative

In contrast to the HR/HP forum model, after initial identification of potential participants, this initiative is completely voluntary on the part of the targeted individual, and their family/ whanau. Participants usually have complex needs and the information sharing requirements include sensitive and personal information. All information sharing is done with the informed consent of the participant. Close co-ordination of multiple agencies, both government and non-government, is required.

The following table summarises the match between the research criteria for selection and this case study:

Prog	Indiv/ FAR	Complex Problems	Govt/Non-govt	Ethnic var	Vol/Comp	Information Sensitivity	Tech
POI	**Indivs and their families**	**Offending history; income; employment; housing; mental health; complex family interactions.**	**Govt**	**Maori**	**Vol**	**Personal; Health; Mental health; Family matters; offending history**	**Low**

(5) Electronic Monitored Bail (EM Bail)

EM Bail is applied for by remand prisoners wishing to spend their pre-trial period at home with electronic monitoring. Authorisation is given to NZ Police to carry out comprehensive checks on the individual to ascertain their suitability for the programme. Police act as the single point of assessment, but share and obtain information on the individual from a broad range of agencies and individuals within the community (e.g. employers, family members).

The following table summarises the match between the research criteria for selection and this case study:

Prog	Indiv/ FAR	Complex Problems	Govt/Non-govt	Ethnic var	Vol/Comp	Information Sensitivity	Tech
EM Bail	**Indivs**	**Offending history; income; employment; housing; mental health; complex family interactions.**	**Govt**	**Pan-ethnic**	**Vol**	**Personal; Health; Mental health; Family matters; offending history**	**Med**