
A. Miriam B. Lips

School of Government and School of Information Management, Victoria University of Wellington, Wellington, New Zealand

Rose R. O’Neill

State Sector System Development, State Services Commission, Wellington, New Zealand

Elizabeth A. Eppel

School of Government, Victoria University of Wellington, Wellington, New Zealand

Improving cross-agency information sharing is at the heart of service transformation efforts to provide more effective services to individuals with complex social needs. So far, however, there is not much empirical research available on cross-agency information sharing. This article explores New Zealand-based cross-agency information sharing practices, with a specific focus on information sharing enablers and barriers in multi-agency collaborative initiatives aimed at achieving integrated social service provision. Empirical findings show the importance of personal data protection and trust in cross-agency information sharing in the New Zealand context; a distinction being made between “hard” and “soft” information; agencies having different information needs and requirements; clear differences in information sharing practices and procedures between agencies with a public service mandate and those with a public safety mandate; the contribution of information sharing protocols and co-location to effective information sharing; and information sharing challenges due to issues around data ownership, a lack of technical interoperability, and a lack of technical capability and knowledge. Generally, in line with operational practice, existing privacy legislation offers an appropriate “default position” for cross-agency information sharing in managing for shared social outcomes in New Zealand. However, there is a need for additional legal support of information sharing by agencies operating under a public service mandate.

Keywords: cross-agency collaboration, information sharing, New Zealand, integrated social service provision

INTRODUCTION

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.

Individuals dependent on welfare support usually face complex problems with interrelated, underlying causes located in various policy domains, such as unemployment, lack of education, poor health, poor housing, and crime. Traditionally, it is expected that these individuals, such as long-term unemployed, the homeless, refugees, and youth offenders, 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 an individual’s needs, however, increased effectiveness of public service
provision can be achieved by building government support around those interrelated needs. For example, the New Zealand Ministry of Social Development is developing a new client-centered public service approach by meeting the interrelated needs of individual customers through an integrated service response in close collaboration with co-located government agencies and community service providers (Lips et al., 2009). Improving information sharing across government and other organizations involved is critical to support this paradigm shift from organization-centric to citizen-centric government and further enhance the effectiveness of public service provision in the wider social sector.

However, with emerging tensions between required cross-agency information sharing and an individual’s privacy for instance, fundamental citizens’ rights like the protection of privacy and confidentiality need to be taken into account in any substantial changes to public service design (6 et al., 2005; Bellamy et al., 2005). Some policy makers even believe that privacy legislation is standing in the way of any progress towards improved information sharing that will support the transformation of public service provision (Lips et al., 2009).

On the other hand, on the basis of an independent review of the UK Data Protection Act and policy relating to data sharing in the UK, Thomas and Walport conclude 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).

Thus far however, there is not much empirical research available on cross-agency information sharing practices, including the role and interpretation of privacy legislation. Therefore this article will explore the following two empirical research questions within the context of the New Zealand public sector:

1. to what extent and how is personal information on individuals with complex social needs shared and managed across New Zealand government agencies and other organizations?; and
2. what are barriers to and enablers of cross-government information sharing aimed at establishing shared social outcomes in New Zealand?

In order to answer these two questions, we provide an overview of available literature in the field of cross-agency collaboration and information sharing. We then further introduce the research methodology and present the empirical findings of this research. Finally, we provide an analysis of barriers to and enablers of cross-government information sharing in the New Zealand public sector and present conclusions and recommendations.

**CROSS-AGENCY COLLABORATION AND INFORMATION SHARING**

Collaboration efforts of government agencies can be viewed on a continuum of degrees of joined-up government, ranging from informal ad hoc arrangements and information exchanges, to formalized collaborative initiatives on integrated service delivery (Eppel et al., 2008). There is no right answer to the question what is the appropriate level of joining-up (6, 2004). Cross-agency collaboration is not easy, and takes time and additional effort by 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 interrelated 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).

Several authors stress that managing in these cross-agency arrangements is different from the vertical and horizontal management that goes on within organizations, and requires different skills and knowledge (Agranoff & McGuire, 2001; Kickert, et al. 1997; Mandell, 1999). For instance, compared with the conventional hierarchical organization there is no central authority within a network of inter-organizational relations; therefore, facilitative leadership, rather than one based on command and control, is needed. The management focus is on selecting appropriate agencies and resources, shaping the operating context and developing ways to cope with the strategic and operational complexity (Agranoff & McGuire, 1999). Furthermore, in order to achieve a shared policy outcome, managing cross-agency arrangements requires coordinating the strategies of participating agencies with different goals and preferences (Kickert et al., 1997).

A widely acknowledged critical factor for successful cross-agency collaboration is trust (e.g., Rommel & Christiaens, 2009). High trust not only results in a deeper form of collaborative behavior between agencies, it also eases the need for control. This in turn reduces transaction costs and the need for formal contracting (Das & Teng, 2001; Ring & Van der Ven, 1992). Agencies that trust each other engage in joint problem-solving, joint action, and increased information sharing (Dyer & Chu, 2003; Edelenbos & Klijn, 2007; Muthusamy & White, 2005). These agencies especially share tacit information, but also strategically important information allowing partner organizations to learn and to innovate.

Increasingly, improving cross-agency information sharing 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 introduction of new Information and Communication Technology (ICT) applications, systems, or infrastructures. However, with limited available empirical research into cross-agency information sharing, research findings 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: 737). Furthermore, recent societal “crises” involving cross-agency collaborations, such as Hurricane Katrina in the United States or child protection services in the UK, have opened up public debate about the information sharing failings of government agencies. This has led to substantial changes to existing institutional arrangements, such as the creation of new legislation, changes to governance structures and leadership, and the introduction of new information systems (e.g., Bertot & Jaeger, 2008; Peckover et al., 2008; Wetmore, 2007).

One of the few available empirical research projects on cross-agency collaboration and information sharing looked at eight multi-agency arrangements in the UK, situated within policy domains of integrated health and social care, crime reduction, and public protection (Bellamy et al., 2007; Bellamy et al., 2008). In the UK, increased sharing of clients’ personal information has been acknowledged as critically important to cross-government collaborative approaches in the wider social policy domain, especially in such areas as child protection, crime reduction, health and social care, offender management, youth services, domestic violence, and substance abuse. In all these fields, UK Central Government has promoted the increased sharing of client information among local agencies by the publication of detailed national guidance notes, the introduction of model information sharing protocols, and the development of centralized information systems including a national violent and sex offenders database, a national information sharing and assessment tool for integrated children’s services, and a national police intelligence system (Bellamy et al., 2008). This effort towards increased information sharing and the availability of centralized, integrated datasets has been strongly pushed by political attention to a number of high profile media cases where the lack of shared information led to disastrous social outcomes including the deaths of long-term abused children, rapes by sex offenders known to the police, and murders by violent offenders living in the community (e.g., Bellamy et al., 2008; Taylor et al., 2006).

In general, the UK-based research findings show that, with strong political pressure and detailed prescription to increase information sharing, information sharing practice is patchy, even within the same organization (Bellamy et al., 2007; Bellamy et al., 2008). Furthermore, consistency of information sharing is dependent on how discretion is exercised in individual cases (Bellamy et al., 2007; Bellamy et al., 2008). As information sharing decisions need to be taken by individual front-line staff members within detailed national information sharing guidance frameworks and on a case-by-case basis, professionals face continual dilemmas between the risk of “false negative” error judgments (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” judgments (i.e., where action is taken, although it turns out later that the risk was lower than would justify it) (Bellamy et al., 2005: 51).

Generally, the people involved in these cross-agency arrangements show greater confidence that confidentiality would be respected appropriately, than that information would be shared appropriately. For instance, informal practices were used to address gaps, deal with inconsistencies, and reduce bureaucratic transaction costs associated with existing legislation and other forms of formal regulation (Bellamy et al., 2008: 753). The overall conclusion of the research is that deficits in both social integration of public officials in cross-agency arrangements and formal regulation are significant in inhibiting the development of consistent and appropriate information sharing practices across the UK social policy sector (Bellamy et al., 2008).

Generally, the literature points to significant barriers to cross-agency information sharing in organizational, political and legal, and technical domains. Based on an extensive literature review Gil-Garcia et al. (2007: 123–124) provide the following examples under each category:

- **Organizational barriers:** can be located at both the meso-level of the organization and the micro-level of individual employees. At the meso-level, barriers are due to explicit and implicit differences among the organizations participating in a cross-agency collaborative arrangement and include misaligned organizational missions, conflicting organizational priorities, diversity in organizational cultures, lack of funding, limited access to implementation models or guidelines, and a lengthy time frame for the manifestation of organizational benefits. At the micro-level, barriers include resistance to change, different individual agendas and goals, misinterpretation of shared information, and misuse of shared information.

- **Political and legal barriers:** the lack of executive and legislative support, restrictive laws and regulations (e.g., civil service regulations), and the requirement to assure citizens’ privacy and confidentiality.

- **Technical barriers:** incompatibility of hardware or software, mismatched data structures, incompatible database designs, incongruous data and information distribution channels, and conflicting data definitions and different terminology.

**RESEARCH METHODOLOGY**

The overall purpose of this research project was to gain an empirical understanding of existing information sharing...
practices between New Zealand government agencies and other organizations in areas where public officials are dealing with multiple, complex social problems from the viewpoint of the individual, 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 and make recommendations for improving cross-agency information sharing to achieve more effective shared social outcomes.

Acknowledging a lack of empirical knowledge on the extent, forms and ways in which New Zealand government agencies and other organizations are sharing information on individuals with complex social needs, we used case study research methodology to focus on the particularity and complexity of multiple cases in order to understand their development under similar legal circumstances (Patton, 2002). With case studies sampled purposively on the basis of a predefined set of selection criteria, we used a qualitative case study research design to bring a depth of understanding to our work that would enhance reliability, enrich our subsequent analysis, and enhance the external validity and transferability to New Zealand policy and practice of the research findings (Seale, 1999). “Information rich” and illuminative cases were selected which could offer useful, in-depth manifestations of the phenomenon of interest in this study, i.e., cross-agency information sharing practices (Patton, 2002).

Research methods used in each case study were a literature and document study, qualitative interviews with professionals from different levels of New Zealand government agencies and other organizations (e.g., frontline staff, middle management, senior officials, policy makers and legal specialists), and participant observation in cross-agency information sharing meetings. Moreover, three qualitative focus group interview meetings and several feedback sessions with research participants were held to verify and refine the research findings.

Qualitative interviewing begins with the assumption that the perspective of others is meaningful, knowable, and able to be made explicit (Patton, 2002: 341). We used the general interview guide approach to explore, in the course of an interview, a list of themes derived from available literature in the area of cross-government information sharing. The preparation of an interview guide provides subject areas within which the interviewer is free to explore, probe, and ask questions that will elucidate and illuminate that particular subject, and ensures that the same basic lines of inquiry are pursued with each person interviewed (Patton, 2002, p. 343). Discussion topics included “working relationships with partner organizations,” “working relationships with other professionals,” “ways of working,” “interpretation and implementation of privacy legislation,” “interpretation and treatment of ‘sensitive’ information,” and “availability and use of ICT-infrastructures and applications.” In order to obtain a wide variety of information sharing practices within the New Zealand context, we wanted to include case studies with varying information sharing arrangements under the New Zealand Privacy Act, 1993. The New Zealand Privacy 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. Administered by the Privacy Commissioner, the Privacy Act contains twelve information privacy principles dealing with collecting, holding, use and disclosure of personal information.

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). During our research we learned that research participants particularly consider Information Privacy Principle 11 (f) as legal support for information sharing:

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 - (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; . . .

In our sample we also wanted to include both successful and less successful experiences with cross-agency collaboration and information sharing. In talking to agency representatives it became apparent that examples of different practice often can be found under the same policy program, in different locations. We selected eight case studies within the following five cross-government programs:

1. **Multicultural Service Centre for Refugees**: operating under the New Zealand Health and Well-Being Action Strategy, this initiative focuses on providing resettlement services for refugees who have entered New Zealand under the annual Refugee Quota Program.
2. **Integrated Service Response**: This program coordinates social service provision to individual clients with multiple problems requiring government services and interventions.

---

3. **High Risk / High Profile Forums (HR/HP):** This national program covers eight regional forums involving monthly inter-agency meetings held for planning the management of high risk offenders once they are back in the community, including the agreement of release conditions.

4. **Priority Offenders Initiative (POI):** This initiative aims to provide wrap-around services for prolific offenders. Under this program, seven agencies regularly meet and discuss the needs of participants on a case-by-case basis.

5. **Electronic Monitored Bail (EM Bail):** This initiative involves an ankle bracelet monitoring system for individuals awaiting trials. NZ Police personnel assess applications for EM Bail and liaise with other agencies to assess whether a person is safe to be released into the community and how the bail conditions will be met. Approximately 120 people participate in this program and it is operating in every Police District in New Zealand.

Eight qualitative case studies were selected and conducted between January 2009 and May 2009, involving approximately 70 semi-structured interviews with professionals (please see Table 1 for a detailed overview of the selected cases).

**RESEARCH FINDINGS**

Across the case studies, the following clusters of empirical findings could be observed:

- **The importance of personal data protection and trust in cross-agency information sharing practices**

  In general, we found that cross-agency information sharing is happening, albeit not in an open or unrestricted way: when information is shared between professionals, it is shared on a “need to know” basis. Conscious about the need to protect personal information, professionals often use abstracted information to alert colleagues from other service providing organizations about the need to further investigate a particular client. This minimalistic form of information sharing between professionals is justified in terms of ensuring that colleagues know enough to do their jobs effectively and particularly also safely.

  Across the case studies we found strong evidence of an implicit professional code of safety protection. This professional code operates in both formal and informal processes and is extended to other service providers and members of the community. For example, an agency providing residency for prisoners on their release is informally alerted to possible issues that affect the safety of their staff or other residents. 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 that the individual needs a particular medication regime, thereby signaling to staff that this client has a different set of needs.

  In accordance with existing privacy legislation, we found that all examined case studies have clear documented processes whereby individual clients consent to provide particular sets of personal information to an agency for a specific purpose. Furthermore, signed consent forms are used by officials as authorization to share information on the client’s behalf, and to share information about clients with other professionals as necessary to achieve their organizational goals. As a result, cross-agency information sharing is usually done with an individual’s consent unless there is a situation of life and death. If staff are privy to information which endangers the health or safety of individuals, this information is shared regardless of the ethical limitations. These situations are rare but as a research participant pointed out to us: “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.”

  A critical enabler of cross-government information sharing turned out to be trust: all case studies provided 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 organizational status of the individual (e.g., Police Officer, Team Leader, Case Worker) does not necessarily ensure that relevant information is passed on to another professional from a different agency, or even to a colleague from the same organizational unit. An example are the difficulties EM Bail staff have in obtaining case information from Police Case Officers: they are wrongly perceived to be working for the Probation Service, which is part of the Department of Corrections, and are therefore considered “outsiders” who are not entitled to “police information.” On the other hand, however, where professional trust is high, professionals from different agencies share information openly and beyond that which is required by the official parameters of their specific job. We also observed in several case studies 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.

- **Professionals make a distinction between hard and soft information**

Across the case studies we found that front-line staff make a clear distinction between the following types of information:
TABLE 1
Overview of Selected Case Studies

<table>
<thead>
<tr>
<th>Selection Criteria</th>
<th>Multicultural Service Centre for Refugees</th>
<th>Integrated Service Response</th>
<th>High Risk/High Profile Forums (HR/HP)</th>
<th>Priority Offenders Initiative (POI)</th>
<th>Electronic Monitored Bail (EM Bail)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agencies Involved</strong></td>
<td>Over 20 central government agencies, local government departments and NGOs providing services in the fields of housing, income support, education, language skills development, psychological services, employment, and health and welfare services. The initiative has multiple funding sources; actions are monitored by funding agencies.</td>
<td>Coordinated services are provided by government agencies and NGOs. Agencies include Work &amp; Income, Career Services, Housing NZ, Health, and Education. Service providers are co-located in a single office</td>
<td>Department of Corrections (prisons’ management, probation, and psychological services), NZ Police and community service providers</td>
<td>NZ Police, Probation and Prison Reintegration Officers, Housing NZ, Education, Child, Youth &amp; Family, Health, Work &amp; Income</td>
<td>NZ Police and other agencies including Housing NZ, Ministry of Social Development, Child, Youth &amp; Family, Health, and employers. A private company (CHUBB) supplies and monitors the electronic ankle bracelets</td>
</tr>
<tr>
<td><strong>Problem Areas</strong></td>
<td>Housing; health; education; employment; language skills; mental health; resettlement needs</td>
<td>Income support; employment; housing; welfare</td>
<td>Crime; income; employment; housing; mental health; family interactions</td>
<td>Crime; income; employment; housing; education; mental health; family interactions</td>
<td>Crime; income; employment; housing; mental health; family interactions; interactions with local community</td>
</tr>
<tr>
<td><strong>Types of Personal Information</strong></td>
<td>Personal demographic data, health, family/relationship matters</td>
<td>Personal demographic data, health, family /relationship matters</td>
<td>Personal demographic data, health, mental health, family/relationship matters, offending history</td>
<td>Personal demographic data, health, mental health, family /relationship matters, offending history</td>
<td>Personal demographic data, health, mental health, family/relationship matters, offending history</td>
</tr>
<tr>
<td><strong>Characteristics of Client Relationship</strong></td>
<td>Voluntary participation by clients</td>
<td>Voluntary participation by clients</td>
<td>Compulsory participation by clients</td>
<td>Voluntary participation by clients</td>
<td>Voluntary participation by clients</td>
</tr>
<tr>
<td><strong>Ethnic Groups Involved</strong></td>
<td>People from a wide variety of nations</td>
<td>Pakeha, 2 New Zealand Europeans Maori, Pacific Islanders, Chinese, other migrants</td>
<td>Pakeha, Maori, Pacific Islanders, Chinese, other migrants</td>
<td>Pakeha, Maori, Pacific Islanders, Chinese, other migrants</td>
<td></td>
</tr>
<tr>
<td><strong>Information Sharing / Legal Arrangements</strong></td>
<td>No specific arrangement; Health Information Code of Practice</td>
<td>No specific arrangement; Health Information Code of Practice</td>
<td>Information sharing protocol; Health Information Code of Practice Information Privacy Principle 11(f)</td>
<td>Information sharing protocol; Health Information Code of Practice Information Privacy Principle 11(f)</td>
<td></td>
</tr>
<tr>
<td><strong>ICT Infrastructure / Application</strong></td>
<td>No shared ICT infrastructure or application</td>
<td>ICT-based assessment tool developed and used by Work &amp; Income</td>
<td>National database owned by Department of Corrections</td>
<td>NZ Police as lead agency has access to national police database</td>
<td>The electronic ankle bracelet sends a continuous signal via satellite to a monitoring unit linked to a control center</td>
</tr>
</tbody>
</table>

2New Zealand Europeans
Front-line officials operate in a situation in which they 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, professionals make a clear distinction 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 or 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. Officials are particularly aware 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 provides a number of distinct advantages to officials with respect to their personal and professional safety, and the safety of other people.

- **Agencies have different information needs and requirements.**

We also found strong evidence for the fact that information relevant to achieving the shared outcomes being sought in the initiatives under study is not homogeneous in nature. Cross-agency collaboration and information sharing involves a wide variation in information needs of different agencies as well as different policy sector-related information sets. For example, under a multi-sector collaborative arrangement like POI, Work & Income only need to know a person’s current status in relation to a range of variables, such as marital status, number of dependent children, and current address, in order to establish their eligibility for specific benefits. For other agencies involved, such as the NZ Police 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.

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 professionals from different agencies. This immediately affects how information is processed and used. For example, unlike their colleagues from the NZ Police or the Department of Corrections, a Work & Income official may not regard previous criminal offending “relevant” information to making an assessment about current benefit eligibility.

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 Multicultural Service Centre for Refugees, we observed that information requirements of government agencies clash with the cultural norms of refugees. This particular example also reveals that who does what with the information, is as important as the information itself.

Another observation across the case studies was that particular data sets, such as medical records and child protection records, receive special protection: access to these data sets is only allowed for authorized 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 among officials of the same professional group or organization. These particular data sets are recognized 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.

Respondents, however, reported that the difficulties obtaining medical information is the area in which safety issues 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 to professionals tasked with providing them with services and assistance. Without any knowledge of 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 individual clients from receiving services they are entitled to. For example, a
refugee continuously missed appointments: when a home visit was carried out, the person turned out to be a double amputee whose physical ability to participate is compromised, and who needs special support that the providing agency was unaware of.

Furthermore, several respondents reported that many health practitioners are unwilling or unable to cooperate with other professional organizations, citing the Privacy Act as a blanket barrier to information sharing even when there is no sharing of personal details about a client involved. In this respect, information sharing practice was widely variable across the initiatives under study and depended on the attitude of individual practitioners, and the ability of officials to build working relationships with other professionals and across agencies. Respondents also noted that, as the health sector is fragmented and widely distributed in New Zealand, they are often unclear in a cross-agency initiative whom to invite to the table, or whom to contact in order to obtain information with respect to individual clients.

In general, several respondents reported that different agencies have different interpretations of the Privacy Act and how it should be applied. When agencies are working together in horizontal arrangements, these different “vertical” interpretations proved to be a barrier to information sharing. Specific support means for horizontal collaborations, such as the Information Sharing Protocol developed for POI, were seen as very helpful.

- **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 operating under a public safety mandate use Principle 11 of the Privacy Act for sharing critical information with other organizations, agencies with a public service mandate do not have such a legal “back-up” in managing for shared outcomes. 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 with both agencies operating under a public safety mandate, and those 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 members operating under a public service mandate is not to share information.

This default position of not sharing information leads to situations where there is no sharing of “intelligence” between agencies like, for example, Refugee Service organizations about shared clients, or Department of Corrections staff and Work & Income staff about system “rip offs” in the area of income support. In some case studies, we found that 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: for example, in the case of refugees, the fact that many refugees can’t meet the eligibility criteria for income support, has implications for their housing situation.

In cases where critical information sharing is not happening, professionals are sometimes exposed to danger without their knowledge. An example is a female official from a service-providing organization not knowing that an inmate has a criminal history of assault on female officers. In the case of the Integrated Service Response initiative, the default position of not sharing information between agencies and the lack of a legal back-up for sharing critical information leads to a situation where clients themselves need to join-up service providers in order to meet their complex needs: as clients need to pass on their referral form, including their personal information, to the agency concerned, they control the information provided to the various partner organizations involved in a collaborative arrangement.

As a result of consistently using signed consent forms as an authorization from the client to share personal 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 organizations. 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 organizations and therefore do not want 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.”

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 as enabling them to share critical information with other professionals and, with that, as the embodiment of this professional code of safety protection. While Principle 11 was regarded as an enabler for cross-agency information sharing, respondents were clear that this is only done on a “need to know basis” among professionals attempting to achieve the same outcomes. In this respect, information sharing that includes 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.”

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 is not applicable, we observed that the same implicit professional code of safety protection is applied among 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 behavior 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 this decision, one interviewee further clarified: “If staff break the law, they do it for the right reasons.”

- Information sharing protocols and co-location support effective information sharing

Respondents reported that having an information sharing protocol for a cross-agency initiative, has provided clarity to officials of different agencies with varying mandates about how to interpret or apply legal provisions. Another advantage of having an information sharing protocol is that it helps to bring representatives of different agencies around the table build trust and develop critical relationships among professionals. In case studies where an information sharing protocol is in place, professionals treat each other as colleagues, even when someone is employed by another agency: for the purpose of the cross-agency initiative, they are treated as “honorary employees” privy to the same information sets. For example, NZ Police staff members participate in HR/HP meetings with Department of Corrections’ staff and share information about inmates. Similarly, senior managers involved with the two POI case studies 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 program.

However, in the information sharing protocols under study, we also observed some grey areas around the sharing of personal information with community-based service providers (e.g., NGOs). Government agencies often have formal information sharing protocols between themselves, but many other organizations assist with practical needs: to professionals concerned it is unclear what information can be shared with these community-based service providers, and how the Privacy Act needs to be interpreted. In most cases under study, a consent form signed by the shared client overcomes these problems.

Several respondents reported that co-location enhances opportunities to develop relationships with other agencies, build trust among professionals and, with that, share information with other professionals, for instance in cases where there is no information sharing protocol in place. For example, under the Integrated Service Response initiative, co-location of government and non-government agencies means there is information available that otherwise would not have been shared: new shared records are being created which can be accessed by all agencies on site. Although these records are paper-based, the status and quality of these records is questionable: for instance, who owns these records? Which agency is responsible for managing them, ensuring their security and accuracy?

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 checking on the shared records that consent has been given. In the same vein, in one POI case study, respondents pointed out that, 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.

- Cross-agency information sharing challenges emerge due to a lack of technical interoperability or technical capability

Across the case studies we observed that each agency has its own information storing processes including one or more 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 related 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 to compensate for the fact that access to these systems is not allowed to personnel from other agencies. Access restrictions can be based on considerations around information security, but also on the perceived need to own and control the data. Manual work-around techniques include duplication of data and data entry processes, as well as sending and receiving e-mails with sensitive personal data in attachments. For example, because NZ Police personnel participating in the HR/HP forum initiative cannot access the Integrated Management of Offenders System (IOMS) owned by the Department of Corrections, relevant information is sent to them on Excel spreadsheets which they have to manually match against the NZ Police databases. The spreadsheets are then updated manually by the NZ Police officials and sent back to Department of Corrections’ staff, where an administrator cuts and pastes the additional NZ Police updates back into IOMS before the joint HR/HP forum meeting.

In the majority of the case studies, technical solutions to data management across agencies are 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 data sets so that they can be certain of their validity and accuracy. For example, Linwood Service Centre staff have designed their own “shared workspace” concept on paper and see such a technical solution as...
highly desirable. However, there are significant difficulties in respect to 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.

In several cases we observed 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 prioritize technical training or systems or hardware upgrades with the limited funding we do have. Unless someone is willing to provide us time and expertise on a voluntary basis we just muddle along doing what we have always done.

Because issues of information security and technical information sharing options are not well understood, we found 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., the NZ Police in POI, the Department of Corrections in the HR/HP forum initiative). This situation 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.

ANALYSIS OF BARRIERS AND ENABLERS OF CROSS-GOVERNMENT INFORMATION SHARING IN NEW ZEALAND

In comparing these research findings with available literature on barriers and enablers of cross-agency information sharing, the following observations can be made.

Unlike the situation in the UK, where information sharing practice is patchy and with a strong political focus on increasing information sharing, the New Zealand research findings demonstrate that information is shared minimally and on a need to know basis. Instead of attempts to increase the sharing of client-related personal information with other agencies, professionals are conscious about the need to protect personal data of individuals and consequently use abstracted information to alert colleagues from other service providing organizations about the need to further investigate a particular client. This minimalist form of information sharing between professionals is justified in terms of ensuring that colleagues know enough to do their jobs effectively and safely, and is an important enabler of cross-agency information sharing in the New Zealand context, therefore.

Furthermore, unlike the UK research findings (Bellamy et al., 2005, 2007, 2008), the New Zealand research findings do not support a deficit in formal regulation in the sense that it would be a significant inhibitor for the development of consistent information sharing practices: information sharing happens across the New Zealand public sector on the basis of an implicit professional code of safety protection, even when it means that staff, in their perception at least, need to “break the law” in order to protect personal, professional or community safety interests. However, New Zealand agencies operating under a public service mandate have a problem with these information sharing practices, as they lack a legal back-up for their information sharing activities. From this point of view, New Zealand public service agencies are confronted with a deficit in formal regulation, unlike agencies operating under a public safety mandate.

Trust in individual relationships appears to be perhaps the most important enabler for cross-agency information sharing in the New Zealand context. This finding is in line with the UK research findings about deficits in social integration of public officials in cross-agency partnerships, as well as with many studies in the field of successful cross-agency collaboration.

Another important enabler of information sharing in the New Zealand situation is the distinction professionals make between formal and informal information, and the exchange of, and reliance upon, informal information between professionals. Further enablers of cross-agency information sharing in the New Zealand context are the use of information sharing protocols, the use of signed consent forms, and co-location of collaborative partner organizations.

An important New Zealand-based research finding is the fact that, across participating agencies, information relevant to achieving shared outcomes is not homogeneous in nature. This particular finding clearly moves away from the UK Central Government’s information sharing solution to make use of centralized integrated databases. In New Zealand, 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 professionals from different agencies, which influences how professionals process and use information. In some cases, differentiated information needs proved to be a barrier to cross-agency information sharing. Similarly, the fact that agencies have different interpretations of the Privacy Act caused problems for cross-agency collaboration and information sharing at the frontline.

Furthermore, in the New Zealand context, there are barriers to information sharing around particular sensitive data sets, such as health-related information. Not only do these data sets receive special protection from professionals, which is supported by legislative restrictions to cross-agency information sharing, but health practitioners also use the Privacy Act as a blanket barrier to cross-agency collaboration. Other, more technical barriers to cross-agency
information sharing in the New Zealand situation are the lack of technical interoperability across agencies, access restrictions to information systems and ICT-infrastructures for staff from other agencies, and issues around ownership of information. A further barrier to cross-agency information sharing in the New Zealand context, which is not referred to in the literature, is the lack of knowledge among partner organizations about available technical solutions for information sharing.

CONCLUSIONS AND RECOMMENDATIONS

The empirical findings from this research show that New Zealand officials are conscious about the need to protect the personal information of clients and are acting upon this need: they share information on a “need to know” basis, rely particularly on soft information as opposed to hard information, and use signed consent forms as authorization to share information with other agencies, for instance. Privacy values are strongly embedded in the way that professionals work and, with that, shape cross-agency information sharing practices. Consequently, in line with operational practice, existing privacy legislation appears to offer an appropriate “default position” for cross-agency information sharing in managing for shared social outcomes in New Zealand.

However, there are clear differences in information sharing practice and procedure between agencies operating under a public service mandate, and those with a public safety 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 organizations 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 vulnerable individuals with complex social needs, leads to ambiguous situations around information sharing and personal data protection in dealing with other government agencies and community service providers. As a result, professionals working under a public service mandate experience legal uncertainty about whether, and if so, what information can be shared with other organizations, and therefore often decide not to share information.

This particular outcome 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. For these reasons we conclude that there is a need for additional legal support of information sharing by agencies operating under a public service mandate, similar to the working of Principle 11 under the Privacy Act for agencies with a public safety mandate. Moreover, having an information sharing protocol supports professionals in focusing on a clear commitment to a shared outcome, developing relationships with other agencies, building trust among professionals, and providing clarity about the application of legal provisions. As information sharing is strongly related to trust in relationships with other professionals, we further recommend using information sharing protocols to improve cross-agency collaboration and information sharing in managing for shared social outcomes in New Zealand.

REFERENCES


