Data Availability and Use
Productivity Commission
GPO Box 1428
Canberra City ACT 2601

29 July 2016

SUBMISSION TO THE PRODUCTIVITY COMMISSION ISSUES PAPER: DATA AVAILABILITY AND USE 2016

Submission Authors	
Judy Allen Honorary Fellow Faculty of Law University of Western Australia 35 Stirling Highway Crawley WA 2009	Carolyn Adams Senior Lecturer Macquarie Law School Macquarie University North Ryde NSW 2109

This submission will focus on the availability and use of data for research, an issue identified in the Productivity Commission Issues Paper, *Data Availability and Use*, as of interest (the Issues Paper).[1] The Issues Paper notes that 'it can be difficult for researchers to obtain administrative datasets for use as empirical evidence'.[2] The authors agree that this is a problem, given the demonstrated public interest in allowing researchers to access and use administrative data collections for research. Such research can, as stated in the Issues Paper, provide insights into the effectiveness of existing public policies and programs and an evidence base for the future development of such policies and programs.[3]

This submission focuses particularly on issues relating to access and linkage of personal information held by governments such as individual health information, education and justice records. This kind of data cannot be provided without very careful protection of privacy but those protections are possible and need not unnecessarily impede the beneficial use of the data. The regulatory processes must be efficient, meaningful and transparent to achieve this balance.

Our submission is based on our experience in the following capacities.

Judy Allen

- Legal academic at the Law Faculty, The University of Western Australia, teaching health law and conducting research focusing on privacy and consent in health research;

1 Productivity Commission, *Data Availability and Use*, Issues Paper (2016) 8.
2 Ibid.
3 Ibid, 9.

- Chair of the Department of Health WA Human Research Ethics Committee;
- Consultant to the Population Health Research Network;
- Delivering PHRN Ethics and Data Linkage Training Workshop to ethics committee members nationally.

Carolyn Adams

- Legal academic at Macquarie Law School, Macquarie University, teaching international human rights law and conducting research focusing on open government, access to government information and privacy;
- Member of the Macquarie University Human Research Ethics Committee (Human Sciences and Humanities);
- Member of the Ethics, Privacy and Consumer Engagement Advisory Group (2009–2014) to the Population Health Research Network (PHRN).

This response is confined to the issues raised in the Issues Paper relevant to our expertise and is in part based on two articles co-written by the authors of this submission and published in 2014. For more detailed treatment of some of the issues referred to below, you may wish to consult these journal articles.[4]

QUESTIONS ON COLLECTION AND RELEASE OF PUBLIC SECTOR DATA

What are the main factors currently stopping government agencies from making their data available?

Complexity of regulatory environment

The current legal framework for access to personal information held by government agencies for research is very complex. This complexity leads to uncertainty and conservative decision making by data custodians and impedes access to data. The absence of clear legal authority has meant that some research projects have been unable to proceed because the release of personal information was unlawful and some projects have been delayed for years while legislative amendments were enacted. Unfortunately researchers have sometimes interpreted this as lack of support or obstruction by data stewards/custodians, however, the data stewards/custodians must operate within the constraints of the applicable law.

The release of personal information for research attracts three bodies of law:

- Statutory duties of confidentiality—Information collected by government agencies under statutory powers can only be used or disclosed for the purposes authorised by the statute and must be treated as confidential.[5] The relevant statutes often also contain express statutory duties of confidentiality;
- Common law or equitable duties of confidentiality—personal information collected in the course of service delivery will usually attract an equitable duty of confidentiality and may also be the subject of contractual duties;

4 Carolyn Adams & Judy Allen, 'Government Databases and Public Health Research: Facilitating Access in the Public Interest' (2014) 21 *Journal of Law and Medicine* 957; Carolyn Adams & Judy Allen, 'Data Custodians and Decision-Making: A Right of Access to Government-Held Databases for Research?' (2014) 76 *AIAL Forum* 11.

5 *Johns v Australian Securities Commission* (1993) 116 ALR 567 at 575; (1993) 178 CLR 408 at 424.

- Privacy legislation—applicable privacy legislation regulates the collection, use and disclosure of personal information by government entities.

Clear statutory authority is required before the use and disclosure of personal/identifying information is lawful. If this is not in place then the disclosure of identifying information will be in breach of the common law or equitable duties of confidentiality and is also likely to breach statutory duties of confidentiality.

In some jurisdictions reliance is placed on the research exceptions in the applicable privacy statutes, however, these provisions do not provide the unequivocal statutory authority that is needed. The drafting of the relevant research exceptions appears to merely create an exception to the new duty created by the privacy principles in the privacy statutes and does not provide the positive authorisation that would support a defence to a breach of an equitable or statutory duty of confidentiality.

An alternative source of statutory authority is in the separate statutes that empower the collection of data for the particular data collection. Many of these statutes are very old, however, and do not support the contemporary approach to maximising the beneficial use of government held data or recognise the privacy protecting practices that are now available. Many do not provide the statutory authority that is needed. Attempts have been made to amend the relevant statutes to accommodate research use of data and data linkage but this piecemeal approach is slow and inefficient and maintains the variability between the empowering statutes. This variability promotes uncertainty and increases transaction costs.

The preferable approach would be a single-purpose statute in each jurisdiction directed to facilitating and regulating the research use of data and data linkage. Such a statute should address both (a) the creation of linkages and (b) the extraction and provision of data. To achieve the certainty that is needed to facilitate research use of data and data linkage the legislation needs to include the following elements

Linkage

- The provisions should apply to all information, including personal information, held by all agencies in the jurisdiction.
- The provisions should operate despite any other law (statutory or common law).
- They should provide authority for data stewards/custodians of all government held data collections to release identifying linkage variables (eg names, birth dates, addresses) to recognised data linkage units for linkage.
- They should authorise the data linkage unit to use and keep this information for data linkage and to maintain enduring linkages.
- The recognised data linkage units should include all data linkage units that meet recognised standards of security and quality and include those in other jurisdictions. This will facilitate cross jurisdictional linkage.

Extraction

- The statute should also provide authority for data custodians/stewards in all agencies to extract and release data to researchers and other approved users.
- This authority must include the release of personal information. Some projects require information that is potentially identifying. For example research involving neonates may need full birth dates. This reflects the approach in the various research exceptions set out in privacy legislation around Australia, which allow the disclosure and use of identified personal information without consent for research where appropriate safeguards are in place.
- The provisions should operate despite any other law (statutory or common law).

- The authority to release data for research or data linkage should be limited by appropriate criteria to ensure that community and individual interests in privacy are well protected and balanced against the public benefit from the use of the data and should be conditional on approval by a Human Research Ethics Committee (HREC) using appropriate guidelines.
- A duty of confidentiality should be imposed on any person receiving the information, such as researchers.

We discuss a proposal for a possible national model to ensure jurisdictional harmony below at page 11-12. This model proposes a unified national legislative scheme, that is adopted and adapted by each jurisdiction.

Cost of meeting data requests

The provision of data to research users is not cost free. The provision of this service needs to be recognised in departmental budgets and staffing and in the job descriptions of data custodians. Supporting data users and maximising the beneficial use of data should be reflected in performance indicators. This is consistent with recommendations of the Senate Select Committee on Health Sixth Interim Report, *Big Health Data Australia's Big Potential* (the Senate Select Committee Report).[6]

What criteria and decision-making tools do government agencies need to help them decide whether to release public sector data for the purposes of research?

The release of government data for research should be premised on an open government framework including the principle that public sector information is a national resource that should, wherever possible and appropriate, be made available for community access and use.[7] The criteria for release of data and the decisions of data custodians should conform to best practice administrative law principles, which regulate government decision-making and aim to ensure that such decisions are being taken in the public interest. Good decision-making by government agencies in matters of public interest should have the following characteristics: consistency, fairness, transparency and timeliness. We note that the Senate Select Committee on Health has recommended that 'each Australian Government agency that is a data custodian develop and publish on its website guidance for researchers detailing its process for data requests and approvals'[8] and the authors would support this as a first step.

The decision-making criteria and tools used in freedom of information (FOI) and public sector information (PSI) regimes provide instructive models for decision making around release of government information in the public interest, including release of data to researchers. Although far from perfect in practice due in part to enduring cultural and resource issues, these regimes provide a framework that aims for consistent, fair, transparent and timely decisions about release of information.

---

6 Senate Select Committee on Health, Parliament of Australia, *Big Health Data: Australia's Big Potential*, Sixth Interim Report (2016) rec 14.

7 Office of the Australian Information Commissioner, *Principles on Open Public Sector Information* (2011).

8 Senate Select Committee on Health, above n 5, rec 8.

A number of elements that generally form part of FOI and PSI regimes could be adapted and applied to decision making by data custodians including: creating a regime in which release is the default position; clear criteria for decision-making, including the factors that may or may not be taken into consideration; timelines for decision-making; a requirement to give reasons for decisions; an independent external review process; and an articulated costs framework. Each of these is considered briefly below. Some of these elements have been specifically addressed in the Senate Select Committee Report including timeframes for decision making and access to review.[9] The authors of this submission would argue, however, that a framework for good decision making should be put in place as soon as possible and not, as the Senate Select Committee recommends, in five years time.

Openness: The most important element of a pro-disclosure regime is the presumption of openness. The OECD *Recommendation for Enhanced Access and More Effective Use of Public Sector Information*, for example, emphasizes maximising access to government information based on the presumption of openness as far as possible.[10] The premise of FOI legislation is that the community has a right to information in the hands of government unless there is a clear public interest in protecting the information from disclosure. The premise of PSI regimes is that information in the hands of government is a valuable economic and social resource that can be enhanced where the information is shared and re-used.[11]

Thus, the default position under FOI and PSI regimes is that information should be released. Currently, the default position in relation to data collections containing personal information is much more conservative, that is, that the data should not be released in order to protect privacy. However, where a research project has been reviewed by one or more HRECs and found to meet relevant standards, including privacy related standards, the default position should be to release the information to the researcher and the onus should shift to the data custodian to articulate and defend any countervailing public interest preventing release.

Criteria: It is important to provide clear criteria to guide data custodian decision-making. FOI regimes, for example, often include inclusive lists of the most important factors that may or may not be taken into consideration in making a decision on whether to release information. Criteria help to ensure transparency and consistency in decision-making. It is particularly important to ensure that data custodians are making decisions based on the public interest and not on the basis that research results may not reflect well on government policies and programs. There is research that indicates that this may happen on occasion.[12]

The federal *Freedom of Information Act 1982* makes explicit that the fact that release of information could cause embarrassment or a loss of confidence in the government must not be taken into account in decision making. The relevant criteria for data custodian decision making should be the subject of consultation with stakeholders and should make clear that protecting government policies and programs from potential criticism is not a legitimate reason for refusing access to information.

9 Senate Select Committee on Health, above n 5, rec 14.

10 Organisation for Economic Co-operation and Development, *Recommendation for Enhanced Access and More Effective Use of Public Sector Information*, C(2008)36, 1172nd sess (30 April 2008).

11 Ibid.

12 Yazahmeidi, B & Holman CD, 'A Survey of Suppression of Public Health Information by Australian Governments' (2007) 31 *Australian and New Zealand Journal of Public Health* 551.

Often the point of the research is to examine the effectiveness of government policies and programs and the results of this kind of research, whether positive or negative, is clearly in the public interest and can be used to improve existing policies and programs or develop new ones.

Timelines: Predictable timelines for decision making by data custodians are essential to support research projects that are often publically funded with research grants that are time limited. In this context, long delays in seeking approval from data custodians can become de facto refusals. There are reports of delays of up to two years before a decision is made by relevant data custodians.[13] Both FOI and PSI regimes recognise the importance of timeliness in decision-making and impose time limits on decision makers. The European Union *Directive on the Re-Use of Public Sector Information*, for example, provides a default timeframe of not more than 20 days, with a possible 20 day extension for large or complex requests.[14]

Reasons: The giving of reasons for decisions is a fundamental requirement of good administration and one of the pillars of Australian administrative law. Both FOI and PSI regimes require that decision makers provide written reasons where access to information is denied, linking the denial to the relevant criteria for decision making. The provision of reasons allows the applicant to identify any errors in the decision; to reconsider and resubmit an application; or seek review of the decision where necessary.

Review: An avenue of independent, external review of administrative decisions is designed to drive greater consistency, fairness and transparency in decision making. FOI regimes generally include access to independent external merits review. Both the OECD PSI Recommendation and the EU PSI Directive discuss the importance of providing an avenue of appeal where access to information has been denied. There is no obvious place for researchers in Australia to seek merits review of the decisions taken by government data custodians. Such decisions are not reviewable in the federal Administrative Appeals Tribunal and access to judicial review is limited. Researchers may be able to complain to an ombudsman in circumstances that amount to maladministration but this does not necessarily provide a constructive model of engagement between data custodians and researchers.

At the federal level in Australia, external review of decisions by data custodians might be placed with the Office of the Australian Information Commission and with equivalent offices at the state and territory level.

Costs: The collection of data by governments incurs a cost and providing access to that data for researchers also comes at a cost. However, the re-use of the data collections for research adds value, while underutilisation of existing data collections is an opportunity lost.[15] Both FOI and PSI regimes emphasise that the costs of access should be kept to a minimum, recognising the public interest in providing access. The OECD PSI Recommendation states that where access is not provided free of charge, charges 'should not exceed marginal costs of maintenance and distribution'.

---

13 Xafis V et al, 'Legal Impediments to Data Linkage' (2011) 19 *Journal of Law and Medicine* 300, 301.

14 *Directive (EC) No 2003/98 of the European Parliament and of the Council of 17 November 2003 on the Re-Use of Public Sector Information* [2003] OJ L 345/90.

15 Australian Association of Gerontology, 'Australian Association of Gerontology Position Statement: Standardising Access to Administrative Datasets on Aged Care Programs for Research Purposes' (2010) 29 *Australasian Journal of Ageing* 185.

The costs of providing data collections to researchers, including working with data-linkage units to de-identify information are significant. It is important to ensure that agencies are appropriately funded and supported to meet the costs of maximising the utility of the data. The Senate Select Committee on Health has recommended that 'the Government review the cost of data access and linkage work undertaken by Commonwealth entities with a view to facilitating research and innovation in the national interest' and that 'the relevant government agencies give greater priority to, and adequately resource, their data custodians' and the authors support those recommendations.[16]

Integrating FOI and Privacy Frameworks

Canadian legislation dealing with privacy and FOI is also of interest in the research context. In Australia, it is not possible to apply for access to data collections of personal information for research under the FOI regimes because these regimes strictly limit access to the personal information of third parties. Section 47F of the *FOI Act 1982* (Cth) provides, for example, that a document is conditionally exempt from disclosure under the Act if it would involve the unreasonable disclosure of personal information about any person (including a deceased person). While this is not an absolute bar to release of third party personal information there is no suggestion in the FOI Act that it contemplates the release of whole data collections of personal information for the purposes of research.

However, it is possible to request access to information for research under the Canadian federal *Access to Information Act* (RSC 1985, cA-1) and this is expressly contemplated in the legislation. Section 19(2)(c) of the Act provides that the head of a government agency may disclose records containing personal information where the disclosure is in accordance with section 8 of the *Privacy Act* (RSC 1985 c P-21). Section 8(2)(j) of the *Privacy Act* allows personal information to be released for research or statistical purposes if the head of the agency is satisfied that certain conditions will be met, for example, that the person requesting the information has provided a written undertaking that the information will not be subsequently disclosed in a form that would allow individuals to be identified.

Although there is a research exception included in privacy legislation across Australia, this link between privacy and FOI is not made in Australian legislation. This is why in Australia, as in many other jurisdictions, researchers don't use the FOI regime to seek access to data collections of personal information. If the FOI legislation in Australia was linked to the research exception in privacy legislation, as has been done in Canada, it would mean that those elements of the FOI regime discussed above—such as a default to openness; criteria and timelines for decision making; a requirement for written reasons and access to external merits review—would also be available to data custodians and researchers. In order for this scheme to work, however, it would also be necessary to ensure that the legislation regulating the various data collections expressly authorised the use and disclosure of the data for research and for data linkage, as discussed above at page 3.

What specific government initiatives (whether Australian Government, state, territory or local government, or overseas jurisdictions) have been particularly effective in improving data access and use?

The development of data linkage capacity in Australia has made it possible to bring together rich sources of data from public and private sources and across jurisdictions. The National Collaborative Research Infrastructure Strategy has supported the development of nationwide linkage infrastructure by the Population Health Research Network. The development of the best practice

16 Senate Select Committee on Health, above n 5, recs 11 & 17.

protocol for data linkage has meant that the use and disclosure of personal information has been significantly reduced both in research projects and increasingly in government use of information for business purposes. The separation principle adopted by these facilities minimises the access to identifiable data and enables data analysts to use whole of population unit level data which is de-identified. Strengthening data linkage capabilities improves the power of the data for beneficial use and also decreases the need to use personal information.

QUESTIONS ON DATA LINKAGE

Which rules, regulations or policies create unnecessary or excessive barriers to linking datasets?

The legal framework

The creation of the linkage map utilizes identifiers from each of the data collections to be linked. Data custodians are required to release the identifiers (eg name, address, birth date) to the data linkage unit. Statutory authority is required for this linkage process to avoid breaching duties of confidentiality. Where enduring linkages are routinely created and are used for multiple purposes including business uses then this stage cannot clearly be described as research. The research provisions in the relevant statutes do not provide clear authorisation for the routine disclosure of identifiers for linkage. Explicit statutory authorisation is required as described in our proposal at page 3 of this submission.

Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs 2008

The Medical Benefits Scheme and Pharmaceutical Benefits Scheme data collections are particularly important in health related research as they contain the largest population-level collections of primary care data and pharmaceutical prescribing data. They are particularly valuable in evaluating the effectiveness of health policies and can be linked to rates of emergency department attendance, hospital admissions and patient health outcomes to analyse the effectiveness and efficiency of health service delivery.

The information in these collections is sensitive personal information and is protected by privacy provisions under the *National Health Act 1953* (Cth) and subject to the rules issued by the Australian Information Commissioner under Section 135AA(3), the *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs 2008.* The current wording of the Guidelines is creating uncertainty about whether it is permitted to link the MBS data and PBS data for planning, monitoring, evaluation and research. This is a serious impediment to the accurate analysis of the provision of health care in Australia.

In order to resolve the uncertainty it is recommended that the Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs be amended to:

- Authorise the disclosure of identifiers from the MBS and PBS data collections for data linkage; and
- Authorise the ongoing storage of the identifiers and linkage map in the data linkage unit.

We note that the Senate Select Committee on Health has recommended that 'the government review the operation of section 135AA of the *National Health Act 1953*, with the aim of improving access to de-identified MBS and PBS data for the purpose of health policy evaluation and development as well as research undertaken in the public interest' and that the *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs* 2008 be reviewed.[17]

17 Senate Select Committee on Health, above n 5, recs 4 & 5.

Destruction of links or enduring links

There are two alternative approaches to data linkage. The first is the ongoing maintenance of enduring linkages. This is most cost effective since it avoids the constant repetition of the linkage process and results in the constant improvement of the links. It does not provide any additional privacy risks where the linkage is conducted and housed in secure facilities. The second approach is to create new linkages for each project and destroy the links after the data is extracted. This has obvious costs in the repetition of work and does not provide justifiable gains in privacy.

QUESTIONS ON ACCESS TO PRIVATE SECTOR DATA

What principles, protocols or legislative requirements could manage the concerns of private sector data owners about increasing the availability of their data?

Private sector data owners such as private health research organisations or private health care providers must comply with two bodies of law if they provide data for research and linkage;

- Common law or equitable duties of confidentiality; and
- Commonwealth, state and territory privacy legislation.

Where no consent is obtained they risk breaching the duty of confidentiality. As discussed above at page 2 of this submission there is doubt that the research exceptions in the privacy statutes provide the necessary statutory authority for a defence to a breach of confidentiality. There is also doubt that they extend to release of identifiers for routine linkage. Appropriate statutory provisions are required to clarify these issues.

QUESTIONS ON PRIVACY PROTECTION

How can individuals' and businesses' confidence and trust in the way data is used be maintained and enhanced?

Community trust in the use of personal information collected by government is promoted by oversight and transparency. This is particularly important where sensitive personal information, such as health information, is collected and used without individual consent. Public awareness and understanding of the collection and use of data is low but the public do strongly support the use of data with proper protections.[18] Human Research Ethics Committee (HREC) review plays an important part in maintaining this community trust. The role of the HREC is valued by consumer representatives and also by data custodians to ensure that interests in privacy are properly evaluated and weighed against the community interest in the beneficial use of the data. Thorough ethics review of new linkages and all research projects should be supported.

Our experience in conducting training workshops on ethics review of data linkage projects for members of HRECs across Australia has made it clear that there is generally a poor understanding amongst ethics committee members of how data linkage works. Without this understanding the ethics review of data linkage projects is likely to be inconsistent and unpredictable. Specialist HRECs to review access to government data for research have been established in some jurisdictions such as WA and NSW. The Department of Health WA, for example, is a specialist HREC with particular expertise, training and experience in the ethical review of data linkage projects. It includes extra members with special expertise in technological security and the management of government data

18 *Collection and Use of Personal Health Data: Exploring the Public Perceptions and Attitudes*, 2006, Synovate, commissioned by DOH WA.

collections as well as research members with experience in the use of administrative data and linked data.

HREC review should be as efficient as possible and multiple reviews should be avoided. There have been significant advances across Australia in achieving mutual recognition of single ethics review for clinical trials. Similar arrangements amongst HRECs with specialist capacity to review these projects are needed for data based research.

We note that the Senate Select Committee on Health has recommended that 'the government take a whole-of government approach to streamlining the ethics approval process and the authorising environment…. [and] work with the States and Territories to establish a national accreditation system so that ethics approvals from accredited jurisdictions are recognised by the Commonwealth.'[19]

Are further changes to the privacy-related policy framework needed? What are these specific changes and how would they improve outcomes? Have such approaches been tried in other jurisdictions?

Harmonisation of privacy principles

The authors support the recommendations in the Australian Law Reform Commission (ALRC) report, *For Your Information: Australian Privacy Law and Practice*, that the privacy principles and key definitions in privacy legislation across Australia should be unified.[20] If the Australian Privacy Principles were adopted as national unified principles, this would eliminate much of the inconsistency and resulting confusion for data custodians across Australia and would greatly facilitate cross jurisdictional research and linkage.

In relation to the definition of 'research' for the purposes of the research exception in privacy legislation, the authors also support the ALRC's recommendation that the research exception in privacy legislation should not be limited to public health research and should extend to cover human research more generally.[21] The research exceptions in other jurisdictions, including the United Kingdom, Canada and New Zealand, are expressed more broadly. For example the Canadian *Privacy Act*, discussed above, applies to use of personal information 'for research or statistical purposes'. There is a demonstrable public interest in other areas of human research, such as education, sociology and criminology, which also have the potential to lead to evidence based policy and program development. These areas of research are also subject to HREC oversight. The ALRC notes in its report that 'research increasingly involves multi-disciplinary approaches, that non-health information is often crucial to health and medical research and that, in any event, it is sometimes difficult to define what amounts to health and medical research and what does not.'[22] The authors of this submission support that view.

Harmonisation of guidelines for HRECs

Under both Commonwealth and state privacy legislation HRECs are charged with the responsibility of reviewing and authorising the use of personal information for research without consent. A single

19 Senate Select Committee on Health, above n 5, Rec 9.

20 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) rec 3–4.

21 Ibid, rec 65–2.

22 Ibid, [65.40].

research project can involve information held by Commonwealth, state and territory government agencies as well as information from private organisations. The HREC considering an application for waiver of consent for such a project is required to apply multiple sets of privacy guidelines as well as the relevant provisions of the *National Statement on Ethical Conduct in Human Research* (*National Statement*) on Ethical Conduct in Human Research on waiver of consent. National collaboration in research is expanding, particularly in the field of epidemiological research and the complexity of the task facing our committees is increasing. Under the current regime a HREC could be required to apply six or more different sets of guidelines to the review of a single project.

The Commonwealth *Privacy Act 1988* alone currently requires research ethics committees to apply two sets of guidelines, the s95 and s95A guidelines, where both Commonwealth agencies and private organisations are involved. This distinction was maintained in the amendments in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth). Our experience indicates that there is no difference in the matters relevant to a waiver of consent for research using information held by Commonwealth agencies and private sector organisations.

We strongly recommend that the Commonwealth lead the development of a single set of guidelines for HRECs to apply in considering a waiver of consent for the use of personal information for research. Uniform guidelines should be adopted by all jurisdictions for both public agencies and private organisations and should be reflected in the *National Statement*. This would significantly reduce confusion for researchers and the burden on HRECs.

The National Statement on Ethical Conduct in Human Research

There are some particular problems with the application of the current provisions on waiver of consent in the National Statement. The waiver provisions are expressed as criteria, all of which must be satisfied, before a waiver of consent is approved. This is not the approach adopted by the privacy statute guidelines or more generally by the National Statement which usually describes principles and matters that should be considered by researchers and HRECs. This is problematic given the difficulty with some of the criteria, for example:

- ☐ The speculative nature of criteria 2.3.10(d) – 'there is no known or likely reason for thinking that participants would not have consented if they had been asked'; and
- ☐ The inappropriateness of requiring HRECs to address the complex legal question required by 2.3.10(i) - 'the waiver is not prohibited by State, federal, or international law.'

The National Statement on Ethical Conduct in Human Research currently provides inadequate guidance on the ethical use of data for research. Chapter 3.2 currently deals with the establishment of databanks; however guidance is required around the use of data more generally. We understand that the Australian Health Ethics Committee is currently reviewing this chapter. We suggest that guidance should be given on assessing and minimising risks to privacy including:

- ☐ Ensuring that identifiable data is only used when it is necessary;
- ☐ Minimising the amount of identifiable data collected;
- ☐ Minimising the number of people that have access to identifiable data, for example, through role separation;
- ☐ Ensuring that researchers only collect and use the data necessary for the project (for example, year of birth instead of full date of birth); and
- ☐ Ensuring an adequate plan for the management and security of the data.

The definitions in chapter 3.2 of the National Statement relating to identifiability of data need to be revised to ensure consistency with the definitions in state and Commonwealth privacy legislation. The risk to individual privacy in the collection, use or disclosure of information depends on the likelihood that the identity of a specific individual can be ascertained. The degree of identifiability must be assessed in relation to each person or organisation which holds the information. It relates to a particular holder of the information and is not an intrinsic property of the information. The identity of individuals may be ascertainable by one person or organisation but not by another. Factors relevant to the degree of identifiability of data include:

- ☐ The type of information held;
- ☐ The quantity of information held;
- ☐ Other information known to the person who holds the information; and
- ☐ The skills and technology of the holder.

How could coordination across the different jurisdictions in regard to privacy protection and legislation be improved?

In 2016, Carolyn Adams (one of the authors of this submission) jointly authored a research report to the Royal Commission into Institutional Responses to Child Sexual Abuse.[23] The report deals with the legal framework for sharing information relating to child sexual abuse between government agencies and non-government organisations, and across jurisdictions, to allow institutions to work together in an integrated way to identify, prevent and respond to institutional child sexual abuse. The aim of the research was to identify elements of the legal framework that were likely to facilitate or, alternatively, impede appropriate and timely sharing of information.

The fragmentation and complexity of federal, state and territory privacy laws are often cited as posing a challenge to the sharing of information that might largely be addressed if jurisdictions adopted a consistent set of privacy principles, as suggested by the ALRC in 2008 and discussed above.[24] As this has not happened to date, coordination across the different jurisdictions in regard to privacy protection and legislation is achieved in different ways in different sectors.

In the early childhood services sector a unique national regulatory scheme is in place that excludes the operation of state and territory privacy legislation in relation to the scheme, and amends and applies the *Privacy Act 1988* (Cth) as a law of each participating jurisdiction. This creates a national, consistent privacy framework for the sector.

The *Education and Care Services National Law* (National Law) and the *Education and Care Services National Regulations* (National Regulations) establish the regulatory structure for education and care services provided on a regular basis to children under 13 years of age, including most long day care, family day care, outside school hours care, and pre-schools and kindergartens across Australia. The National Law was originally passed as a law of Victoria in 2010 and has been subsequently adopted by corresponding legislation in each state and territory. It is intended to establish 'a jointly governed,

23 Adams, C and Krista Lee-Jones, *A Study into the Legislative—and Related Key Policy and Operational—Frameworks for Sharing Information Relating to Child Sexual Abuse in Institutional Contexts* (Report for the Royal Commission into Institutional Responses to Child Sexual Abuse, Sydney, 2016).

24 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008).

uniform and integrated national approach to the regulation and quality assessment of education and care services'.

Section 5 of the *Education and Care Services National Law Act 2010* (Vic) provides that the *Privacy and Data Protection Act 2014* (Vic) does not apply to the *Education and Care Services National Law* or the instruments made under that law. This provision is replicated in other jurisdictions with appropriate reference to the relevant state or territory privacy legislation.

The National Law establishes a clear framework for information sharing between relevant agencies and across jurisdictions in the early childhood services sector. Part 13 of the National Law sets out the circumstances in which disclosure may, must or must not occur. The National Law imposes a general duty of confidentiality on those exercising functions under the law, but also makes it clear that the duty does not operate if the information is disclosed in the exercise of functions under or for the purposes of the National Law or where the disclosure is required or authorised by any law of a participating jurisdiction and in a range of other circumstances.[25] The National Law also establishes a specialist Office of the National Education and Care Services Privacy Commissioner.[26]

These arrangements provide another possible model for sharing data more seamlessly across institutional and jurisdictional boundaries. The model does not compromise privacy protection as the federal Privacy Act continues to apply. It does, however, remove the real and perceived barriers thrown up by the complex web of federal, state and territory legislation relevant to data linkage. It also expressly addresses concerns about common law and equitable duties of confidentiality by providing express statutory authority for use and disclosure of personal information under the National Law and Regulations.

25 *Education and Care Services National Law Act 2010* (Vic) sch s 273.

26 Ibid, sch s 263.