NSW INJURY RISK MANAGEMENT RESEARCH CENTRE

DATA CONFIDENTIALITY AND PRIVACY POLICY

1.0 INTRODUCTION

The NSW Injury Risk Management Research Centre (the Centre) was officially established in September 1999 when a Deed of Agreement (the Agreement) was signed by its four funding partners - NSW Health, the Roads and Traffic Authority (RTA), the Motor Accidents Authority (MAA) and the University of New South Wales (UNSW). The Agreement contained specific clauses concerning the purpose of the Centre, the obligations of the funding partners and data confidentiality. As part of the Agreement, the funding partners were obligated to provide copies of their data to be used for injury research purposes by the Centre and to allow their data to be stored in the Centre's data repository. A new funding agreement was signed in May 2003. The issue of confidentiality was covered in clause 21, page 16 of the new Agreement and reads:

> ***The Centre acknowledges that during the course of providing the Services to the partners it may become acquainted with or have access to information owned by a partner which the partner wishes to keep confidential and the Centre agrees to maintain the confidence of the confidential information and to prevent its unauthorised disclosure to or use by any other person, firm or Company without the consent of the relevant partner first being obtained.***

In order to maintain the confidential nature of these data and future data collections, either for the core research program or for other research funding agencies, the Centre has developed this privacy policy after reviewing the following documents:

- Australian Institute of Health and Welfare Act 1987, Section 29, Confidentiality
- Commonwealth ***Privacy Act 1988, Information Privacy Principles***
- NHMRC ***Guidelines Under Section 95 of the Privacy Act 1988***
- NHMRC ***National Statement on Ethical Conduct in Research Involving Humans***, 1999
- Joint NHMRC/AVCC ***Statement and Guidelines on Research Practice***
- NSW ***Privacy and Personal Information Protection Act***, 1998 (PPIP)
- HRIP Act – ***Health Records and Information Privacy Act, 2002***
- NSW Health's ***Information Privacy Code of Practice,*** Second Edition December 1998
- For Section 6 (Linkage of administrative datasets), advice from the NSW Privacy Commission, 2002

2.0 DEFINITIONS

Authorised Research Scientist- Staff or Student of the Centre authorised to ***collect and/or analyse*** Personal Information for research purposes of the Centre and who has been trained to ***collect and/or analyse*** Personal Information in an ethical manner

Authorised User- user granted permission by the Centre to access ***existing*** Data, usually only IRMRC Authorised Research Scientist

Centre- NSW Injury Risk Management Research Centre

Code of Conduct- document detailing measures designed to protect the confidential nature of Personal Information and Data obtained or held by the Centre and which all IRMRC staff and students are required to sign and abide by

Confidentiality Agreement- document detailing measures designed to protect the confidential nature of information obtained from the Centre which all collaborators and Third Party users of the IRMRC data resources are required to sign and abide by (yet to be developed)

Consent- permission obtained from an Individual to collect Personal Information about them

Data- unit record data currently held by the Centre

Individual- any person who is contacted for the purposes of obtaining Personal Information for a research project conducted by the Centre

Partner- one of the four centre core funders - NSW Health, the Roads and Traffic Authority (RTA), the Motor Accidents Authority (MAA) and the University of New South Wales (UNSW)

Personal information- any information or an opinion about a person whose identity is apparent (unique identifying information) or can reasonably be ascertained from the information or opinion (potentially identifiable information). Unique identifying information include items such as name and address, photographs, biometric information including fingerprints and genetic characteristics, will always be Personal Information.

Potentially identifiable information includes a range of other information that can also become personal information, if it is viewed in combination with other information, which together are sufficient to allow a person's identity to be 'reasonably ascertained'. Items/characteristics which may fall into this category include age, date of birth, ethnicity and diagnosis. The potential for these types of general information to become identifying is higher when dealing with a small population, or dealing with unusual or rare clinical conditions.

Secure Environment- secure data server and storage cabinet maintained in a locked office in the Centre that can only be accessed by Authorised Users

Staff- person directly employed by, or working at, the Centre

Student- person undertaking a research project at the Centre for educational purposes, under the supervision of senior Centre staff

Third Party- person or organisation who is not an Authorised User

3.0 DATA COLLECTION

1. In cases where Personal Information needs to be collected for lawful research purposes of the Centre, the information will be limited to a minimum set of variables needed for the research project.
2. Ethical approval to collect Personal Information will be sought by the Centre before proceeding with any research project.
3. Personal Information from an Individual will only be collected by, or under the direction of, an Authorised Research Scientist, using fair and lawful means.
4. The Authorised Research Scientist will obtain informed Consent from the Individual before attempting to collect Personal Information and if Consent is not obtained, the Authorised Research Scientist will not proceed, unless prior ethics approval has been granted to waiver the need for this Consent.
5. As part of obtaining an informed Consent, all Individuals will be provided with information detailing the following:
    - the purpose of the collection
    - any laws authorizing the collection
    - who will use the Data
    - how an Individual's Data can be requested once it has been collected
    - how the confidential nature of the Data will be maintained
    - the Centre's policy for providing data to third parties.
6. The Authorised Research Scientist will inform the Individual that they may withdraw from the project at any time.
7. Once Personal Information from an Individual is collected by an Authorised Research Scientist, it will become Data and will be protected by the terms in the following sections.

4.0 DATA SECURITY

4.1 Confidentiality

1. All Authorised Research Scientists and Authorised Users will be required to sign a Code of Conduct before proceeding with any of the following:
    - collecting Personal Information or accessing Data
    - analysing Personal Information or Data or
    - disseminating results from the analysis of Personal Information or Data.

4.2 Storage

1. All Data held by the Centre will be maintained in a Secure Environment.
2. The Centre will maintain a list of Data containing Personal Information.

4.3 Access

1. In cases where Personal Information is collected for research purposes of the Centre, access will be limited to Authorised Research Scientists, Authorised Users who are involved with the project and the Individuals, who will be able to access their own data.
2. Only Authorised Users will have access to Data. The Data will be obtained using a username and password.
3. Student Authorised Users must be directly supervised by senior Centre Staff and must obtain prior approval for data access for their specific project by submitting a formal request for such access though the Centre's Quarterly Review Committee.
4. Authorised Users who are Students will only have access to the Data directly relevant to their project.
5. Third Parties may be granted access to summarised data that does not violate Clause 21 of the Agreement establishing the Centre and clause 4.1 of this Privacy Policy. However, provision of this summarised data to Third Parties may be subject to costs, as specified in the Centre Costing Policy.
6. Per clause 21 of the Agreement, requests from Third Parties who wish to access unit record Data held by the Centre, but owned by a Partner, will require written authorisation from the Ppartner before requested Data can be released. Once authorisation is given by the Partner and agreed to by the Centre, the Third Party will be required to sign a Confidentiality Agreement before requested Data can be received. Once Third Parties have signed the Confidentiality Agreement, they will be considered Authorised Users.
7. Requests from Third Parties who wish to access unit record Data collected and owned by the Centre only require authorisation from the Centre. Once authorisation is given by the Centre, the Third Party will be required to sign a Confidentiality Agreement before requested Data can be received. Once Third Parties have signed the Confidentiality Agreement, they will be considered Authorised Users.

4.4 Disposal

1. The Centre will hold all Data used for trend analysis for 20 years, after which time it will be archived and stored in de-identified format.
2. The Centre will hold all Data collected for research projects for seven years, after which time it will be disposed.
3. Data will be disposed in a manner that renders individual Data records unreadable and prevents reconstruction in whole or in part.

5.0 DATA USE

5.1 Research

1. In cases where Personal Information is collected for research purposes of the Centre, the information will be used only in the manner for which it was intended.
2. In cases where Personal Information is collected for research purposes of the Centre, it cannot be modified except when the Authorised Research Scientists corrects an inaccurate data record. If Personal Information in any record is modified, a note will be attached to that record describing the modification, the date of this change, and the person who made it.

5.2 Reports

1. In cases where Personal Information is collected and analysed for research purposes of the Centre, the information will be reported in a manner that prevents the identification of any subject.
2. In cases where existing Data is analysed, the information will be reported in a manner that prevents the identification of any individual. The manner of reporting will be the following. In general, data will not be released where there are five or fewer cases per cell in a data table or figure (i.e. the 5 cell rule). This is based on the premise that, due to the small numbers involved, it may be possible to identify the identity of one or more of the reported cases, and/or the statistical significance may be affected. As this general rule may not protect the identity of individuals in all cases, a judgement needs to be made in all cases on the adequacy of this rule to ensure individual privacy and confidentiality. Alternative approaches should be used where there is any doubt, including:
    - making the data cover a wider field (e.g. aggregating data across a number of council areas such as on a regional basis); or
    - providing only an overview of data rather than specific details.

6.0 LINKAGE OF ADMINISTRATIVE DATASETS

The Privacy Commissioner has taken the view that use of Personal Information is necessary for research for the purposes of prevention of, or amelioration of the effects of, injury then it is clearly in the public interest to promote such research. However, it is also recognised that the use of identified data also has the effect of enhancing the data collected, particularly when it can be linked to other sources. Enhanced data is more valuable and hence there is a greater risk of the information being used outside the bounds of the original research project.

In the case of linkage of administrative datasets, Personal Information is used to identity data subjects in at least two sets of data, each of which contains personal identifiable information. The two sets of data are cross-matched and, where it can be ascertained that the two data sets relate to the same individual, an enhanced data set can be formed. Once the enhanced data set is formed, it is de-identified for the purpose of further use and distribution as part of a research project. The University is judged to be a suitable agency for conducting such a cross matching exercise and holding the resulting data sets, as its sole interest is for research.

Other agencies may have potentially wider interests in the information and there is an associated risk that the information will be used for other purposes. Any such data linkage needs to conform to the current directives of the NSW Privacy Commissioner.

The current (2003) directives are summarised as follows:

6.1 The Centre should, wherever possible, be responsible for producing and retaining the `enhanced' data as it has no further interest in the enhanced data, other than for addressing the ***a priori*** stated research purpose/s. Other Partners who provided the data potentially have a greater use for the data, if it can enhance their own data collections.

6.2 The proposed research must be an approved research project where a research ethics committee has specifically approved the collection from a third party. This would then allow:

- the principle that collection of Personal Information be directly from the individual or guardian to be modified to allow collection from third parties or other agencies participating in the research proposal, so long as the research ethics committee has specifically approved the collection from the third party
- the principle that use must be directly related to the purpose for which it was collected to be modified to allow for use for approved research project purposes

- disclosure of non-sensitive Personal Information may be made to:
    - an agency or agencies identified in an approved research project (defined at Part 2 of the Draft Code) or to a supervisor or assessor of that project; and
    - an entity which can assist in the research but which was not named specifically in the research proposal as long as they are subject to any other conditions of approval.
- disclosure of sensitive Personal Information is allowed without the consent of the Individual where:
    - the disclosure is in accordance with a protocol approved by a research ethics committee, subject to conditions considered appropriate by the committee not to disclose sensitive Personal Information without the consent of the Individual or their closest survivor and the researcher has agreed to be bound by these conditions; or
    - where the research project is approved on the basis that the research committee has considered the National Statement (particularly Part 18) which specifically relates to the research project and the conditions identified in 4.2.3 (e) (i),(ii) & (iii) are satisfied. These relate to the practicality of seeking consent, the balance of public interest in the proposed research and privacy considerations and there being adequate safeguards against disclosure that would result in harm to an individual or individuals concerned or their survivors.
    - the research designer will need to determine whether the research includes 'sensitive information'.

6.3 The proposal must be consistent with the current PPIP Act or relevant Code of Practice and should include a Privacy Impact statement containing:

- a statement as to why the use of identifiable data is necessary for the effectiveness of the research as the use of identifiable data potentially raises the value of the data in terms of use and disclosure.
- a statement in the research design detailing:
    - which agency is responsible for conducting the data matching;
    - the length of time that the agency can maintain any set of personalised data obtained in the cross matching process, and in particular the 'enhanced' data;
    - how the matched data will then be de-identified before use or disclosure for research.
- A statement detailing whether or not it is practicable to gain consent from the subjects. Where practicable, a letter should be sent to the subjects by the agency which holds primary data outlining the following:
    - why is it necessary to use Personal Information to conduct the research;
    - which agencies hold Personal Information which will be used in the project;
    - how they may access information about themselves;
    - how long their Personal Information will be retained; - what will happen to their Personal Information;
    - that the Personal Information is subject to confidentiality agreements between the parties but legally such confidentiality may not always be protected (e.g. if required under subpoena or warrant or under some other legal requirement); and
    - where possible, seeking their consent.

6.4 Contracts and protocols for linkage research projects will bind parties so that use and disclosure outside the terms of the research project can only be made:

(i) where lawfully authorised to do so under the PPIP Act; and

(ii) where compelled by law to do so.

6.5 Agreements between the University and any participant who obtains new Personal Information (including enhanced Personal Information) as a result of the research should include specific clauses with respect to the need to ensure that Personal Information is only used and disclosed for purposes outlined in the research proposal. This would entail inclusion of the following clauses:

- no uses can be made outside the terms of conducting the research project;
- disclosures outside the terms of the research project only be made:
    - where lawfully authorised to do so; and
    - where compelled by law to do so (such asunder the terms of a subpoena, warrant or court order);
- any breach of these conditions constitutes a breach of contract; and - any breach of these conditions may be a breach of the PPIP Act.
- any requests received by the participating agencies, including for internal use other than research, for new Personal Information obtained through the research project (including requests by law enforcement agencies) must be advised to the Centre. The Centre will be responsible for ensuring compliance with the PPIP Act.