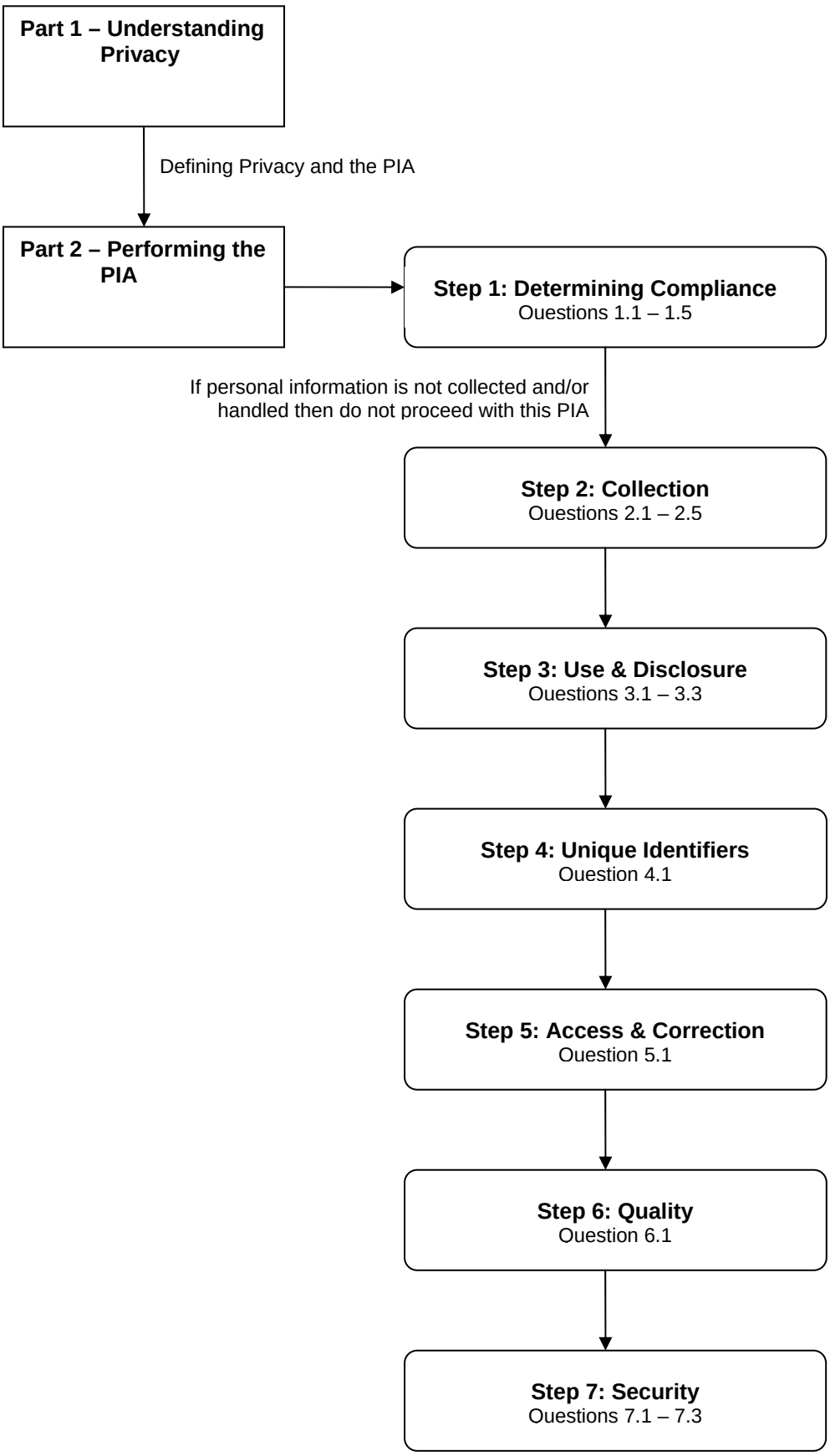
Privacy Impact Assessment (PIA) Guide Human Ethics Applications

An assessment tool to identify risks with respect to the privacy of research participants

SUMMARY – PRIVACY IMPACT ASSESSMENT (PIA) GUIDE



PART 1 – UNDERSTANDING PRIVACY

Introduction

In August 2004, the Office of the Victorian Privacy Commissioner released a guide to developing privacy impact assessments (PIA) as a means for organisations to identify and address privacy issues of current or proposed actions.

A PIA identifies risks in respect to the privacy of individuals, which if left untreated may cause distress. From an organisational perspective, a PIA facilitates compliance with privacy laws and promotes confidence by all stakeholders involved in the assessment process.

This PIA identifies risks with respect to the privacy of research participants.

Further assistance regarding this PIA can be obtained from the University's Privacy Officer by email: **Privacy@latrobe.edu.au** or tel. **(03) 9479 2060**.

Defining Privacy

Privacy is about controlling who knows what about individuals by protecting their personal information (commonly referred to as information privacy). This involves the establishment of rules governing the collection and handling of personal, sensitive and health information[1].

Personal Information

Put simply, if recordable information can reasonably identify an individual, or if their identity is apparent, then it is considered personal information

Health Information

This applies to:

1. Health information that is personal information collected by an organisation.

2. Any personal information or an opinion collected or used about an individual in providing a service in health, mental health, disability, aged care, or palliative care.

Sensitive Information

This is information, or an opinion, about an individual's –

- Racial or ethnic origin; or
- Political opinions; or
- Membership of a political association; or
- Religious beliefs or affiliations; or
- Philosophical beliefs; or
- Membership of a professional or trade associations; or
- Membership of a trade union; or
- Sexual preferences or practices; or
- Criminal record.

[1] Please refer to **appendix 1** for complete definitions.

In terms of a research project, information privacy may cover:

- A name on a consent form;
- Responses to questions in a survey form that can be used to identify a participant;
- Sound or film recording of group sessions where participants identify themselves or identity is relatively easy to ascertain; or
- A data set that includes de-identified data but can be readily re-identified with cross matching to another set of data.

Why Privacy?

Privacy has long been regarded as part of liberty and a human right. Article 12 of the Universal Declaration of Human Rights states –

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour or reputation. Everyone has the right to the protection of law against such interference or attacks."'

Research participants expect their privacy to be protected.

Research participants who believe their privacy has been breached can make formal complaints.

Respecting and protecting privacy enables investigators to gain trust and confidence from research participants.

Gaining trust and confidence enhances the reputation of a research project.

PART 2 – PERFORMING THE PIA

Complete steps 1 to 7 by referring to the questions provided. Each question has been explained to assist users of this PIA to further understand privacy considerations.

Step 1: Determining Compliance

Respecting privacy requires responsible collection and handling practices in accordance with applicable laws. These laws include:

- Information Privacy Act 2000 (Victoria);
- Health Records Act 2001 (Victoria); and
- Privacy Act 1988 (Federal).

These three Acts are broadly similar, particularly their intention to protect privacy, and all have their origins in the OECD's (Organisation for Economic Co-operation and Development) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

1.1	**Does the project involve the collection and/or handling of personal information?** **Yes (Continue)** **No (Do not continue)**	The starting point is to determine whether the project requires this Privacy Impact Assessment (PIA). If the project does not collect and/or handle personal information then there is no need to perform any further assessment.
1.2	**Does the project involve the collection and/or handling of sensitive and/or health information?** **Yes (Go to 1.3)** **No (Go to 1.4)**	It is important to know if sensitive information or health information is being collected because this form of information may have specific requirements under privacy laws. For example, collecting sensitive information from participants will usually require consent unless otherwise permissible under privacy laws.
1.3	**Is the project intending or claiming to provide a health service as part of the research?**	If the project is providing a health service to participants then the project is deemed a health service provider and may be subject to specific privacy requirements. For example, the participant may request the project investigator(s) to provide their health information to another health service provider or request another health service provider to contact the project investigator(s) to request such information. Refer to **appendix 1** for a complete definition of a health service.

1.4	**Are any project investigators from the private sector or a jurisdiction outside of Victoria?**	It is important to understand the location(s) of investigators to establish privacy jurisdiction and responsibility. For example, if an investigator is operating from outside Victoria then it will be important to ensure their commitment to privacy laws is similar to that of La Trobe University. This commitment may come in the form of a law, binding scheme or contract which stipulates compliance with privacy laws similar to those to which La Trobe University must comply.
1.5	**Will the project be using a contracted service provider to collect and/or handle personal information?**	If a contracted service provider is used to collect and/or handle personal information then it is important to establish in a contractual agreement a clause that will bind the contracted service provider in much the same way, and to a similar extent, as La Trobe University is bound to comply with privacy laws. The **University's Legal Services Unit** can assist.

Step 2: Collection

2.1	**Is it necessary for the project to collect personal information?**	Assessing the necessity to collect personal information should be based on an assessment as to whether it is unavoidable for the project. Necessity is also dependent upon practicality. Consider whether other alternatives are available in collecting information that will not reasonably establish participant identity. For example, can the project use de-identified information? Can the project perform collection anonymously?
2.2	**What opportunities (if any) will the project provide participants to consent or decline in the provision of certain types of personal information?**	Providing participants with a clear understanding of the collection process and having them involved as much as possible (that is, having a 'say') facilitates collection in a fair and open manner. For example, the project's information sheet, explanatory statement, or consent form may provide details to participants as to what aspects of their personal information they can decline in providing.

2.3	**Will the project inform participants of the following matters regarding the collection of their personal information?** ▪ **Identity of the project and how to contact the project** ▪ **Purpose of collecting their personal information** ▪ **Uses and disclosures (if any)** ▪ **Right to access and correct their personal information**	When collecting personal information, it is necessary at or before the point of collection (or if not possible then as soon as practicable after) for the project to inform participants of certain matters in order to enable collection by fair means. Informing participants of such matters concerning collection of their personal information may be performed through a consent form, information sheet, or explanatory statement used by the project. The University has a guideline on constructing privacy statements. These statements can be included in the project documentation. This guideline is available at: **http://www.latrobe.edu.au/records/privacyltu**
2.4	**Will the project collect personal information directly from the participant or indirectly from someone?**	If reasonable and practicable to do so, the project must collect personal information about participants directly from the participants. If personal information about participants is being collected from someone else (such as a collection agency) then reasonable steps must be taken to make participants aware of matters outlined in **ref.2.3**. Consideration in undertaking reasonable steps will include: ▪ The degree of difficulty in making contact with participants and making them aware of such matters; ▪ Whether the original collecting agency can advise participants about the project's use of their personal information; ▪ The nature of the information; and ▪ Importantly, whether making participants aware of such matters would pose a serious threat to the life or health of any individual. A project cannot absolve itself of responsibilities it would have in the collection of personal information from an individual by getting that same information from someone else.

2.5	**If the project is collecting personal information from someone else then does that someone else have authority to disclose personal information to the project?**	For example, the other party may have approval from their organisation's Human Research Ethics Committee for disclosing the personal information. Alternatively, the other party has obtained consent from individuals in disclosing their personal information. It is important to retain evidence of this authority.

Step 3: Use & Disclosure

3.1	**Why is personal information being collected from participants?** **In other words, what is the purpose of collection?**	The project needs to establish the main purpose for collecting personal information from participants and to state this purpose in a manner that is meaningful to participants (see **ref.2.3**). When defining the main purpose, it is important to consider the position of the participant by asking "What do they think they are providing their personal information for?" Participants will typically not have a detailed understanding of the project so it is important to convey the purpose in a manner in which they understand. Always remember this rule - *Use and disclose personal information only for the purpose for which it was collected. If use and disclosure is not for the purpose of collection then make sure it is permissible under privacy laws*
3.2	**Will the project use and disclose personal information collected from participants only for the purpose in which it was collected?**	If other uses and disclosures are expected then they need to be conveyed to participants, particularly if the uses and disclosures are not related to the purpose of collecting their personal information. For example, if an investigator expects personal information collected from participants to be used by another research project for unrelated analysis and/or research inquiry then this should be conveyed to participants (see **ref.2.3**).
3.3	**If the project was to realise an unexpected use and disclosure of personal information collected from participants, is it possible to seek consent from participants?**	A project may experience a use and disclosure that is not related to the purpose in which personal information was collected from participants. If this is the case, consent from participants to perform use and disclosure is the best way to comply with privacy laws.

Step 4: Unique Identifiers

4.1	**Will the project assign unique identifiers to participants used by another organisation for the same individuals?**	Adopting unique identifiers must be carefully considered by projects due to the potential of data linkage and matching and the ability to profile individuals. These activities are invasive to the privacy of individuals. Using unique identifiers is determined by necessity. Necessity is dependent upon practicality and efficiency of the project not merely a desire for convenience. A safe practice for projects in adopting unique identifiers from another organisation is to seek consent from the participants. Projects assigning unique identifiers to participants used by another organisation for the same individuals must not disclose the same unique identifiers unless consent has been obtained from participants.

Step 5: Access & Correction

5.1	**Does the project have a designated contact for participants to request access and correction to their personal information?**	Participants have a right to access their personal information and seek correction (if established that the information is not accurate, complete and up to date). However, there may be circumstances when a request from a participant to their personal information is denied. For example, providing access may pose a serious and imminent threat to the life or health of any individual; providing access would have an unreasonable impact on the privacy of other individuals; or the request for access is frivolous or vexatious. The project needs to consider how personal information will be maintained to enable ease of access and use. It is important to remember that the right of access and correction by a participant remains as long as the information exists.

Step 6: Quality

6.1	**Will personal information collected by the project be checked (whether at the point of collection or periodically) for accuracy, completeness, or currency?**	Ensuring personal information is accurate, complete, and up to date depends on the following factors: ▪ The nature of the information; ▪ How recently the information was collected; ▪ How quickly the information can go out of date; ▪ Who provided the information; ▪ What the project uses the information for; ▪ How the information will be used by the project; and ▪ Whom the project disclosed the information to. For example, a project may use fixed/static personal information about participants for retrospective analysis so it would not require periodical checking. On the other hand, a project may require procedures to up date personal information about participants if studying these individuals over many years.

Step 7: Security

7.1	**Once personal information is collected by the project, will access and use be limited to individuals within the project based on necessity to perform their roles?**	Less handling of personal information improves greater control and less chance of threats to security whether internal or external. If personal information is used by several individuals within the project then consideration should be given to ways in tracking (or auditing) the whereabouts of the information at all times.
7.2	**Once personal information is collected by the project, will it be moved around or disseminated for further use and access by the project?**	Privacy travels with personal information so it is important to consider what safeguards are needed to protect personal information during movement or dissemination. If personal information is stored and transmitted in electronic form then safeguards may need to include password protection to authorise access. If information is regularly transmitted via the internet then encryption may be a possibility.
7.3	**Do you know how long to retain personal information collected from participants?** **Do you know where to store the personal information in a manner in which it can be accessed and potentially used?**	The best form of securing information is to not hold it. In other words, the project should destroy or de-identify personal information when no longer required by the project. However, La Trobe University has requirements regarding the retention of information in which it is responsible for.

		Refer to **appendix 2** for retention periods pertaining to such information. Personal information must be stored in a manner that can be accessible, retrievable and useable. This can be problematical if those responsible for handling the information during the project are no longer available, or the information is dependent upon a software application or operating system that is no longer used.

Appendix 1

Personal Information

As defined by the Information Privacy Act 2000 (Vic), personal information is –

Information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Sensitive Information

Sensitive information, as defined by the Victorian Information Privacy Act 2000, means information or an opinion about an individual's –

- Racial or ethnic origin; or
- Political opinions; or
- Membership of a political association; or
- Religious beliefs or affiliations; or
- Philosophical beliefs; or
- Membership of a professional or trade associations; or
- Membership of a trade union; or
- Sexual preferences or practices; or
- Criminal record.

Health Information

As defined by the Health Records Act 2001, includes information or an opinion about -

- The physical, mental or psychological health (at any time) of an individual; or
- A disability (at any time) of an individual; or
- An individual's expressed wishes about the future provision of health services to him or her; or
- A health service provided, or to be provided, to an individual -

that is also personal information; or

- Other personal information collected to provide, or in providing, a health service; or
- Other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
- Other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or of any of his or her descendants –

but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act;

Health Service

As defined by the Health Records Act 2001, a health service is defined as –

- An activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the organisation performing it -
  (i) to assess, maintain or improve the individual's health; or
  (ii) to diagnose the individual's illness, injury or disability; or
  (iii) to treat the individual's illness, injury or disability or suspected illness, injury or disability; or

- A disability service, palliative care service or aged care service; or
- The dispensing on prescription of a drug or medicinal preparation by a pharmacist; or
- A service, or a class of service, provided in conjunction with an activity or service referred to in paragraph (i), (ii) or (iii) that is prescribed as a health service –

but does not include a health service, or a class of health service, that is prescribed as an exempt health service for the purposes of this Act generally or for the purposes of specified provisions of this Act or to the extent that it is prescribed as an exempt health service;

Appendix 2

Retention periods applicable to research projects

Activity	Examples of Records	Retention Period
Administration of Research Programs The approval of research projects, management and interim reporting on research progress. Includes the formulation of applications for ethical clearance.	• Applications for ethical clearance • Project approval applications • Project resource allocation • Annual project progress reports • Correspondence with other research groups, research partners or stakeholders • Consent forms	Destroy 7 years from date of last entry
Laboratory/Field Station Administration	• Rosters • Consumable requests • Maintenance rosters/requests • Technical records for equipment or consumables • Instructions for use of facilities	Destroy 7 years from date of last entry
Collection and Analysis of Data Not Involving Clinical Trials The observation, recording and analysis of research results.	• Experimental results/readings • Data sheets • Observations • Field notes • Surveys • Questionnaires • Laboratory note books • Photographs and other recordings of experimental outcomes	Destroy 5 years from date of completion
Collection and Analysis of Data Involving Clinical Trials		Destroy 15 years from date of completion