BOOKLET 23

Griffith University Research Ethics Manual

Privacy and confidentiality in human research

V3.8 July 2020

Contents

1.0 Introduction

In Western liberal-democratic societies, personal privacy is often described as a fundamental human right (though the extent and degree of protection of this right may not necessarily be fully defined in legislation or otherwise codified). Even when respect and protections of this kind are not codified or mandated through regulation, it underpins societal norms and customs.

Paragraph 1.11 of the National Statement (2007, updated 2018) indicates that consideration for personal (and sometimes group) privacy is one of the ways in which the ethical principle of respect for persons is addressed in the design and conduct of human research.

In Australia, the right to privacy was initially articulated for personal information held by Commonwealth agencies through instruments such as the Commonwealth Privacy Act 1988 and financial information protections. In 2001 the Privacy Act was amended to apply to private sector bodies (including businesses) and other organisations (including not-for-profit organisations) with an annual turnover of more than $3 million dollars as well as private organisations providing health services and holding health information. In 2014 the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Privacy Amendment Act) made many significant changes to the Commonwealth Privacy Act. The Privacy Amendment Act now

codifies arrangements with regard to financial disclosures and reporting (e.g. credit checks) that were previously only articulated by an Australian code of conduct. In 2014 that code of conduct was also updated with the release of the Privacy (Credit Reporting) Code 2014. With the release of the (Queensland) Information Privacy Act 2009 (see 4.2) Queensland has enacted the implemented similar privacy principles.

This Act applies to Griffith University. As such, the requirements of the legislation must be met for any research conducted under the auspices of the University (even if that research is to be conducted in another Australian jurisdiction, or even outside of Australia).

The focus of both ethical privacy standards and statutory privacy protections is principally upon the access/collection/generation/receipt/use/analysis/storage/reporting/publication/sharing of identified personal information.

This Booklet offers advice and information relating to both ethical and statutory privacy issues.

Back to contents

2.0 National guidelines

The National Statement (2007, updated 2018) is the Australian reference for human research ethics matters. Paragraph 1.11 **directs that researchers should "respect the privacy, confidentiality and cultural sensitivities of the participants and, where relevant, of their communities. Any specific agreements made with the participants or the community should be fulfilled".**

The issue of privacy is frequently revisited throughout the National Statement principally as an issue of consent (e.g. paragraph 2.2.6(f)). Paragraph 5.1.19 of the National Statement also indicates that one of the responsibilities of institutions is ensuring that there is "due regard for "the relevant privacy regulations" in its non-HREC research ethics review frameworks.

Inset One – I will not be publishing / reporting identified personal information...so do privacy regulations apply to my research?

There is a common misconception that, as long as a researcher protects the privacy of participants when they publish / report the outcomes from the research, then privacy regulations do not apply to that research. This is incorrect.

If a researcher will access / collect / generate or otherwise obtain identified personal information, then privacy regulations apply to that research, even if the individuals will not be named or otherwise be identified in any publications or reports arising from the research.

Additional statutory requirements will also apply if the data will be analysed, stored, reported and/or shared with others in an identified form.

As was noted in the introduction, the national reference for privacy regulation is the amended Commonwealth Privacy Act 1988.

Even though the Australian Code for the Responsible Conduct of Research (2018) does not directly discuss privacy, Principle 5 refers to respect for research participants, as does Researcher Responsibility 18 and Institutional Responsibility 2 discusses compliance with laws. The Management of Data and Information in Research good practice guide includes numerous references to privacy and adherence to privacy regulation.

Back to contents

03.0 Privacy as an ethical consideration

Given the existence of Queensland and Commonwealth privacy legislation (see 4.0 of this Booklet) it is not surprising that researchers and ethics reviewers can focus much of their attention on privacy as a statutory rather than ethical consideration. Such a focus can result in privacy being only approached as a question of what is legally required and what is permissible within the scope of the relevant privacy regulation. However, privacy should also be approached as an important component of the core ethical principle of respect for persons.

There are many compelling reasons for researchers to have due regard for the privacy of potential participants. These include (but are not limited to):

- A view that everyone has a right to limit access to his or her person (Allen, 1997). Such a right encompasses informational, physical and proprietary privacy. Beauchamp and Childress (2001) argued our right to privacy rests on the principle of respect for autonomy. On this basis, while some matters cannot or should not be concealed, people should have the right, as far as is possible, to make decisions about what will happen to them. In the context of research, they should be able to maintain secrets, deciding who knows what about them.

- Paragraph 1.11 of the National Statement directs that researchers (in the design and conduct of human research) must 'respect the privacy, confidentiality and cultural sensitivities of the participants and, where relevant, of their communities. Any specific agreements made with the participants or the community should be fulfilled'. The issue of privacy is revisited later in the National Statement, principally as an issue of consent (e.g. paragraph 2.2.6(f)). Paragraph 5.1.19 also indicates that one of the responsibilities of institutions is ensuring that there is due regard for the relevant privacy regulations in its ethics review frameworks.

- It may be helpful to separate obligations of confidentiality from those relating to privacy. Confidentiality is an obligation that arises in certain relationships or under contract on the recipient of *any* information not to use that for any purpose other than that for which it was given. For example, if a person who provides information a part their participation in a project, that information should only be used for that poject. Researchers typically owe participants such an obligation in relation to the information participants provide as part of their involvement in research. Privacy is an obligation on the holder of *only* personal information (from which a person can be reasonably identified but where the person may not have provided the information) not to use the information for purposes other than those for which it was collected. For example a business may obtain information with personal identifiers as part of a credit checking process, but they cannot use that information for any other process or share it with third parties (such as a researcher). Typically, privacy obligations are owed by institutions to those identified in information that institutions collect and hold. Those obligations need to be addressed by researchers who seek access to that information. For example, express consent should be sought before a researcher is provided the information.

- There may be privacy risks to the participants if their comments, contribution or information became known to third parties. Sometimes there may be similar risks associated with just the fact that an individual has participated in the research or

because they were approached about participating. See Booklet 9 of this manual for more about risks in research, including case studies relating to privacy.

- The fact that a researcher has demonstrated due regard for and care of an individual's privacy and confidentiality can sometimes increase the likelihood that they will elect to participate in a project.
- The fact that a researcher has demonstrated due regard for and care of an individual's privacy can often be beneficial to the candour of the information participants provide for a project (because the participants aren't worried that third parties will have access to their comments/information).
- Concerns about privacy can be a common source of concerns and complaints from participants (or even potential participants) and these can often be the result of insufficient information about how their privacy has been respected and safeguarded.
- Respecting the privacy of individuals can foster an ongoing positive relationship between participants and researchers, which may be valuable long after the current work (e.g. willingness to participate in future studies involving either the same researcher or other researchers).

3.1 Participant anonymity

There is a common misconception that to be considered ethically justifiable a research project must protect the anonymity and/or the confidentiality of participants (e.g. that participants will not be identifiable from the output/publication/reported results of the research). This is not the case.

In fact, there is no ethical standard that demands anonymity for research participants. Indeed, in the case of research in some fields, a proportion of participants would expect to be identified and might only participate in a project if their contribution to the work is to be acknowledged. It might be disrespectful to those participants if they were not identified. In other cases, potential participants will understand they will be identifiable and are unlikely to be vulnerable because of that identification (e.g. a public figure) will realise that they probably will be identifiable in the reporting of results but are well placed to assess the risks and make a decision.

The question of whether participants are to be identified and whether direct quotes or commentary will be ascribed to them may initially be a respect for persons issue, or perhaps more specifically, a consent issue. An explanation of whether (and if so, to what extent) the participatory status of individuals will be discernible by third parties, and the degree to which third parties will be able to link comments/information/other research data to individual participants, should appear in the consent materials. See 8.0 for further discussion on the issue of identification. Refer to Booklet 22 of this Manual for further information about consent.

Related to the consent consideration is whether any identification of participants (their participatory status and linked information about them) could expose them to some form of risk (physical, psychological, social, economic, etc.).

In many cases the researcher(s) will be unable to assess the presence or significance of any risks associated with the identification of participants. Commonly, it is the potential participants themselves who will be best placed to make this assessment. That is one of the reasons why it is

important to ensure that the consent material discusses the issue of identification, so potential participants can weigh the risks and make an informed decision. Refer to Booklet 9 of this Manual for further information about risks in human research.

It is because of these risks, as well as a degree of courtesy, that research designs that will involve direct quotations or ascribable information should have a further mechanism for checking back with the participants to seek their further consent for the use of the quotation or other information about them that will appear in the publication or report arising from the research. See section 8.0 for further discussion with regards to the use of this kind of mechanism.

Of course, there can be situations where third parties (e.g. law enforcement agencies) may seek to compel the release of identified data. You can find further commentary on these matters in Booklet 40 of this Manual.

Commentary Inset 2 – Code keys and re-identifiable information

When referring to information that is re-identifiable a code key will be accessible to the research team. It is a security measure to help safeguard the identities of participants or other third parties and can be an important risk management strategy. In some cases, the code key might be accessible to one or some of the researchers and/or might only accessible at a specified time.

EXAMPLE: A research project involves prisoners keeping a diary about their experiences with a new online simulation tool and commenting on whether they think it useful for their development of work skills prior to their release from a custodial correctional facility. It is a longitudinal study with data being collected over a three-year period. The research team is very conscious that participants might perceive their comments as having an impact on their chances of an early parole and so undermine the candour of their comments. Consequently, a research assistant will collate the data of participants and the other team members will not have access to the code key.

It may be appropriate to destroy the code key at some point (e.g. when all the data has been collected and matched). Ordinarily the code key and data should be stored separately and not communicated/transported together.

Code keys might be used for de-identified data (e.g. a government data group might provide coded information to a research team and not provide them with the code key – so the research team will not be able to correspond information with identifiable individuals). In such cases it might be important to reflect upon the fact that reports back to the supplying department could in effect be personally identified (because re-identification will be possible), even if the researchers cannot identify individuals.

It is often the case that providing potential participants with a clear explanation of the intended approach to confidentiality (rather than a simple promise of confidentiality) can give them confidence in the research and improve the chances that they will decide to participate.

3.2 Privacy states of personal information

Chapter 3.1 of the National Statement discusses the issues related to the identifiability of individuals in data and information collected, used and disclosed for research but does not use specific terms to classify that information, This is because identifiability of information lies on a spectrum and whether individuals can be reasonably identified will depend on the information and the contexts in which it is used.

A single project may involve multiple sets of data, possibly in different privacy states (e.g. anonymous surveys, re-identifiable test results and personally identified interview audio recordings). Also during the course of a project the privacy state of sets of data might change (e.g. client files might be accessed in a personally identified form, they might be analysed and stored in a re-identifiable state, and then reported without any personal identifiers).

The privacy state of personal information will determine the approach required with regard to consent (see 3.3) and whether there are statutory considerations that apply (see 4.0).

3.3 Consent and privacy

When consent is sought from potential participants for the future use of information they provide, whether it is and will remain identifiable is likely to be a central issue for them. Whether the information is or is not identified personal information, consent will usually be one of three forms:

- **specified**, where they are provided the precise details of how their information will be utilised (which might also specify who will have access to their identified information, where it will be stored, how it will be reported and whether it will be shared with others);
- **extended**, where they are provided with more general information about how, whether and by whom the identified information will be used – this is most commonly the case where the information might be of use to more than one project within a particular area or topic; or
- **unspecified**, where potential participants are told only that their identified information might be utilised for other research or educational purposes.

Commentary Inset 3 – Self-coded data

Researchers can sometimes find themselves in a situation where it is important that not only participants be anonymous to other parties (e.g. because of the ethical sensitivity of the topic) but also that not even the researchers can associate the comments or information with an identifiable individual. This can be problematic for some designs (such as longitudinal work) where there is a need to combine information from one person over multiple data points. A strategy that has been successfully used in the past is participant self-coding.

Self-coding involves participants being provided with a formula to construct their own unique code. Two examples might be mother's family name at birth name plus mother's birthdate, or first pet's name and father's birthdate (e.g. harding3011 or parker2809) or some more complex version of this.

Key considerations for the code formula are:

- *the formula does not include information that the researchers or others can easily obtain (e.g. student number, birthdate)*
- *the resulting code is long enough to generate unique codes given the size of the cohort*
- *the resulting code only includes information the participants can readily remember.*

Such coding is not without its limitations (e.g. the kind of example above could be decoded by law enforcement) and some information that might seem easy to remember may not actually be easy for everyone.

The selection of a form of consent and the degree of identifiability of provided information is likely to be determined based on very project-specific matters. It may have impact upon the degree to which individuals are willing to consent to participate in a project (e.g. the specified form of consent may be more successful, especially if individuals perceive risks if their information becomes known to others). Conversely, specified consent might make future use of that information (even by the same researchers) problematic. A single project may involve multiple sets of data with different forms of consent. See Booklet 22 of the GUREM for more about consent and Booklet 42 for more about the retesting/new use of data.

3.3 Responsibilities of researchers

As discussed previously, researchers have important ethical and regulatory responsibilities in designing, conducting and reporting human research. These responsibilities apply to all human research irrespective of the design, discipline, level or funding source.

In summary, these responsibilities are to:

- only collect, access and use identified personal information that is necessary for the research

- obtain consent or waiver of the consent requirement for collection, access and use of personal information
- handle identified information responsibly (including safeguarding against unauthorised access to the information)
- not disclose personal information to third parties without prior consent or ethical authorisation (see 6.0 for more)
- when reporting the results of research or producing outputs of the research, not disclosing the identity of individuals without prior consent or authorisation from the ethics review process (see 6.0 for more).

Back to contents

4.0 Statutory privacy considerations

In addition to the Commonwealth *Privacy Act 1988*, most Australian States and Territories have some form of privacy regulation. In practice, research conducted under the auspices of Griffith University is more likely to be subject to the Queensland regulations (see 4.2) rather than the Commonwealth regulation. The Commonwealth, Queensland and other Australian statutory privacy arrangements describe obligations with regard to the collection, access to, storage and disclosure/sharing of identified personal information. The specific requirements of each State and Territory may vary, and researchers should ensure they are familiar with the needs of each jurisdiction within which they or their team are collecting, storing or using personal information . Additional requirements may exist when moving personal data between countries (such as the regulation relating to the transmission of personal information in and out of the European Union).

4.1 The Commonwealth Act

The Commonwealth Privacy Act is the Australian adoption of principles articulated in documents such as the *International Covenant on Civil and Political Rights* (Article 17) and the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The Act provides protection of personal information held by organisations in the private sector (applying to bodies with a turnover of $3M or more) and all health service providers who hold health information. The Act contains 13 Australian Privacy Principles (APPs) that apply to those bodies that are within the scope of the Act.

Under the framework established by the Commonwealth Privacy Act, personal identified information should ordinarily only be used with the prior consent of the individual to whom the information relates. This consent will normally cover how the information can be used, who is authorised to access the information, and the degree to which the information will be shared with third parties. Such consent requirements do not ordinarily apply to the use of de-identified personal information.

Section 95 of the Act provides for a public interest test, which permits for the use of identified personal information held by a Commonwealth entity for medical research without the consent of the individual to whom the information relates, if approved by a human research ethics committee. A similar test is provided by section 95A of the Act and allows the use of identified

health information for research, or the compilation or analysis of statistics, relevant to public health or public safety, without the consent of the individual to whom the information relates, when approved by a human research ethics committee.

Further information about this test can be found at 4.1.3 of this booklet. Unfortunately, no provision is made for such a public interest test for non-health research.

The APPs articulated by the Act also govern the appropriate storage, use and disclosure of personal information, even if consent has been obtained. See 4.1.1 of this booklet for more about the practical implications of the APPs for human research.

Further information about the APPs can be found on the website of the Office of the Australian Information Commissioner (OAIC).

4.1.1 IMPLICATIONS OF THE COMMONWEALTH ACT

The Commonwealth Privacy Act has direct implications for the design and conduct of human research. It describes obligations with regard to the collection, access to, storage and disclosure/sharing of identified personal information. Additional requirements may exist when moving personal data between countries (such as the regulation relating to the transmission of personal information in and out of the European Union). **The Act does not apply to the access, use or disclosure of information or data that is not personal information, i.e. information from which a person cannot be reasonably identified.**

The practical implications for human research in Australia are:

1) Existing identified personal information can only be **accessed** for research in one of three situations:
   a. with the consent of the individual (whether specified, extended or unspecified – see 3.3)
   b. where the research use is related to the purpose for which the information was collected
   c. where a HREC has waived the consent requirement (see 4.1.2.3)

2) The statutory provisions that allow access to personal information without consent but with HREC approval apply only when using:
   a. personal information held by Commonwealth agencies for medical research
   b. health information held by private entities for research related to public health and safety

3) In circumstances within 1) a. and 1) b., individuals, whose personal information is being collected, must be provided with sufficient material about use, storage and sharing of that information with other parties

4) Personal information should ordinarily (see 5.0) not be disclosed to other parties without the consent of the individuals

5) Researchers in possession of personal information must store and manage it responsibly and in accordance with the consent obtained, the instructions of the individuals, or the directions of the relevant HREC.

Ideally, researchers should obtain the consent of individuals **before** personal information is accessed or used. Alternatively, the information could be accessed and used in a non-identifiable form so that it is no longer identified personal information.

These constraints apply even if a researcher will protect the privacy of individuals in any output arising from the research. For example: a researcher cannot access existing records, containing personal information, for the purposes of extracting data (unless the requirements discussed at (1) above are met) even if the analysis and reporting of the results of the work mean individuals cannot be identified. This is the case even where a researcher has authorised access to, as well as permission to, use the information for a purpose other than research (a researcher may be able to access the name and contact details of students as part of her duties as a lecturer for a course, for example).

These constraints do not apply if the personal information is already on the public record (such as in a published news report – though researchers should reflect upon whether the reported facts are disputed or are themselves a breach of privacy).

In the absence of it being practical to obtain consent from individuals (see 3.3), or where the conditions for a waiver of the consent cannot be satisfied, (see 4.1.2.3) it may be impossible to conduct research with existing personal information.

Commentary Inset 4 – Two possible solutions for research design elements that have been curtailed by privacy regulations

FIRST CONTACT WITH POTENTIAL PARTICIPANTS - The most common strategy is for an organisation that holds the contact details of the potential participants to contact them on behalf of the researcher(s).

Ideally, the potential participants should be invited to contact the researchers directly if they are interested in participating and the organisation should not know the participatory status of individuals (thus diminishing the degree to which individuals might feel under some pressure to participate and perhaps also minimising some potential risks associated with the organisation knowing who has participated).

This initial contact should make it clear that no information about the individual potential participant (including their name and contact details) has been released to the researcher(s).

ACCESS TO RECORDS/FILES IN AN IDENTIFIED FORM, FOR USE IN A DE-IDENTIFIED FORM - There can be situations where a researcher does not need to collect primary data from participants, but is interested in reviewing records/files that perhaps cover an extended period, where seeking the consent of the individuals named in the records/files would be impractical.

Even though the analysis of the data (and so the reporting of the results) will be in a de-identified form, because it is necessary to access the records in an identified form, a statutory privacy issue exists.

The most common solution is for the organisation that holds the records to authorise the researcher to access the records, onsite and under the control of the organisation, and for the researcher to be authorised to extract de-identified information from the records/files for later research analysis.

In effect, the organisation is making the researcher an authorised officer, and is deeming the access to the records and extraction of de-identified data an authorised use.

Alternatively, the organisation can extract from identifiable information, the data items that the researcher needs and provide them in a de-identified form. This will, however, involve the organisation "using" the identifiable information and the lawfulness of this will need to be explored.

Researchers are urged to consult with the Office for Research (see Contacts below) when considering regulatory privacy matters. This may require that the researchers need to modify the design and conduct of their research (see Commentary Inset 4).

4.1.2 APPROACHES TO ACCESSING EXISTING IDENTIFIED INFORMATION

4.1.2.1 Obtaining consent

Prior to the researchers accessing personally identified information the consent of the individuals is obtained. As discussed at 3.2 this consent might be specified, extended or unspecified. One of the practical difficulties for researchers might appear to be that it is impossible to seek consent for access to an individual's personal information without knowing whom to approach. However, it may be possible for the original collector of the information to seek that consent or to seek a waiver of the consent requirement on behalf of researchers. See 4.1.2.3 for more about waivers.

Sometimes, contact details for potential participants are not available because of the time that has elapsed since the data were collected, or if the contact details are not current or were never recorded. On other occasions, contacting the potential participants could be a cause of distress or other risk. Once again, a waiver of the consent requirement may be the only practical solution.

As long as the information is not sensitive personal information (as defined by the Act) the opt out approach might be another valid recruitment/consent mechanism (see 14.5 for more about the opt-out approach.

4.1.2.2 De-identification of data

In situations where it is not possible to obtain prior consent (see 4.1.2.1) and where a waiver of the consent requirement (see 4.1.2.3) is either not an option or not practicable, the only alternative is for the researchers to **access** the data with personal identifiers removed. This can be achieved by coding the data prior to the researchers accessing the information for research purposes in such a way that the researchers cannot identify individuals. See 4.1.2.4 for more on this.

At Griffith University, it is not uncommon for an academic to have authorised access to some personal information (such as the academic records of his or her students) for teaching or administrative purposes. However, this does not mean that he or she has authorisation to access and use that information for research purposes. See 4.1.2.5 for some practical solutions to such a situation.

It can also be important to consider the degree to which non-identifiable data can be linked with other data so that the identities of individual subjects can be determined (see NS Chapter 3.1). Researchers should also consider the degree to which the anonymity of participants can be protected (see 9.0 of this booklet).

4.1.2.3 Waiver of the consent requirement

Researchers should contact the Office for Research (see Contacts) early in their research project to determine whether a waiver of the consent requirement is an option for their research and for advice with regard to applying for a waiver. Such a waiver is different from substituted consent (such as when a patient is unconscious or otherwise unable to express their wishes). See Booklet 28 of this Manual for more about research with such persons.

As noted above, the prior consent of individuals should be obtained prior to access to or research use of their personal information. Where it is not practical or desirable to obtain consent (e.g. because seeking consent may cause individuals distress), the data should be accessed and used in a de-identified form.

Another option available to researchers is to seek a waiver of the consent requirement (see National Statement paragraphs 2.3.9 – 2.3.12). A waiver of the consent requirement for access to or use of identified personal information can only be approved by a HREC (rather than by another body) and must be based upon consideration of a public interest test and specified criteria. If researchers intend to expose illegal behaviour, they will also need to show that the illegal activity bears on the discharge of a public responsibility or the fitness to hold public office (see National Statement paragraph 4.6.1) and that the value of exposing the illegal activity justifies the adverse effects on the people exposed (see National Statement paragraph 2.3.11)

A waiver of the consent requirement can be approved, pursuant to the *Privacy Act 1988* (Commonwealth), for the use of personal information held by a Commonwealth agency for medical research. Medical research is defined only as 'including epidemiological research'. A waiver of consent can also be approved for the use of health information for research related to public health and safety, being information held by State authorities or private entities that provide health services. Health information is understood to mean any information related to the provision of health services. These statutory provisions are often referred to as research exemptions.

Each year institutions must report to the NHMRC on waivers granted pursuant to the guidelines under either s.95 or 95A in the previous 12 months. The National Statement imposes a related obligation on institutions to report publicly on waivers of consent, following completion of research in which the waiver was granted.

The implications of these provisions are:

- A waiver of the consent requirement is **not required** for access to or use of aggregate information or information where the personal identifiers have already been removed.
- A waiver of the consent requirement is not required if the individuals have consented (whether specified, extended or unspecified see 3.3) to the use of their information for research.
- An HREC can approve a waiver of the consent requirement for the use of personal information held by a Commonwealth agency for medical research, and also for the use of health information held by a private entity that provides health services for research related to public health or safety. Institutional reporting requirements apply whenever such waivers are approved.
- Unfortunately, there is no similar waiver provision for the use for research of Commonwealth-held personal information for non-medical research or for use of non-health information held by State authorities or private entities. Accordingly, such information can only be used for research with the consent of the individuals.

4.1.2.4 Other statutory exemptions

There are other Commonwealth statutory exemptions to the requirement that consent be obtained for the use of personal information. For example, the Federal Privacy Commissioner can permit acts that would otherwise breach privacy principles by reaching a public interest determination. However, while such exemptions might apply to medical research they are rare in other disciplinary areas (Public Interest Determinations 5 and 8) and the process can take considerable time and effort.

Specific legislation can authorise such uses by identified government agencies. For example, under the Commonwealth *Student Identifiers Act 2014*, 'Registrars' may disclose personal information about an individual if the use or disclosure is for the purposes of research (s18.2) that:

a. relates (directly or indirectly) to [vocational] education or training, or that requires the use of student identifiers or information about [vocational] education or training; and

b. meets the requirements specified by the Ministerial Council.

4.1.2.5 Practical solutions

Researchers may find themselves in situations where it is not possible to obtain individual consent: before they access the personal information (see 4.1.2.1); where the data cannot have personal identifiers removed prior to access (see 4.1.2.2); and where a waiver of the consent requirement is either not available (because the information is not health information or the work is not medical research) or all of the criteria cannot be met (see 4.1.2.3). We discuss some practical solutions to common privacy difficulties below. When facing such a situation, researchers are urged to consult with their School's REA, who is likely to discuss the situation with the Office for Research (see Contacts).

1. **De-identification by data custodian -** Related to the matters discussed at 4.1.2.2, a de-identification strategy involves the custodian of the data (such as the practicum placement officer for a faculty) redacting material, removing personal identifiers before passing over data to the researchers. The process means that the researchers access the data in a non-identifiable form (see 3.2). In some cases, the data custodian will be willing to extract the information, perhaps using an automated tool to remove personal identifiers from the data prior to it being provided to the researchers. Nevertheless, researchers should be prepared for the possibility that a custodian might be unwilling to do this work. Custodians might consider extracting the data and removing the personal identifiers to represent either a 'use' for a purpose not directly related to the collection purpose or a significant time or resource impost. It may also be impractical for some data/research (e.g. because the information comes from more than one source, the uniqueness of individual cases, or the volume of the information involved). For these reasons, this strategy may not be a viable alternative for all research.

   For example, in *Deitchman v. E.R. Squibb and Sons* in 1984, the manufacturer of the drug diethylstilbestrol (DES) sought all the information contained in the University of Chicago's DES Registry of 500 cases. The Registry refused to breach patient confidentiality and Squibb offered to accept the data stripped of identifying information. The task was described by the Chairman of the Department of Obstetrics and Gynecology at the university as 'herculean' (from Chalmers and Israel, 2005)

2. **Distribution by the data custodian -** Also related to the matters discussed at 4.1.2.2, this strategy can be appropriate for designs such as surveys, links to web-based tests, invites to attend focus groups, and similar designs. Where the data custodian distributes the material on behalf of the researcher, it can be important (e.g. in the consent material) to explain clearly:

   - that the material is being distributed by the custodian rather than the researcher

- whether any identifiable information has been provided to the researcher
- whether the custodian will be aware of the participatory status of individuals.

In addition to mitigating any privacy concerns or worries about risks, the above information might improve participation rates and goodwill between the potential participants and the researcher. Where practicable and relevant for a research design, this strategy can represent less of an impost than the strategy discussed at 1 (above) but still requires the custodian to do some extra work.

3. **Separating roles and authorised access** - In some cases, a researcher may have authorisation to access identified information for one purpose (such as the conduct of a course) but may not have authorisation for access for research purposes. One possible strategy would be for the researcher to access and code, aggregate and/or de-identify the data while 'wearing the authorised hat' so that the information is used for research only once the personal identifiers have been removed. Alternatively, and preferably, the researcher might hand over one of the roles to someone else who has appropriate authorisation but does not have a conflict of roles. A similar strategy should be used when not all members of the research team have authorisation to access the identified information (e.g. the researcher who has authorisation codes, aggregates and/or de-identifies the data prior to sharing it with the colleague who does not have authorisation). In cases such as this it is important to confirm with the relevant custodian that the practice is permitted; carefully explain the strategy to the ethics reviewers (see 5.0); and maintain file notes about the process that was followed.

4. **Custodian seeking consent -** A variant of 1 (above) is where the custodian seeks the consent of the potential participants for them to provide identified personal information to the researchers. Like the approach 1 and 2 this strategy requires time and resources by the custodian, though it may represent less of an impost for them. Like strategy 2 it can be important (e.g. in the consent material) to explain clearly:
    - that the material is being distributed by the custodian rather than the researcher
    - whether any identifiable information has been provided to the researcher
    - whether the custodian will be aware of the participatory status of individuals.
5. **Researcher credentialing by the custodian -** One possible solution to situations where the custodian has limited capacity to undertake tasks such as those described a 1, 2 and 4 (above) might be for the custodian to credential a researcher to come onto site and extract the required de-identified data from the individual records. This can only occur where such an arrangement is not legally precluded and with the approval of the appropriate person (e.g. in a government department this might be a deputy director general). An element of this approval should be a reflection on how this authorised access will be announced or reported and described. The ethics reviewers are likely to utilise the kind of public interest test described at NS2.3.9 and then report publicly that a waiver of the consent requirement was approved for the project. See 4.1.3 for more about the public interest test for waivers of the consent requirement.

4.1.3 PUBLIC INTEREST TEST

A researcher who wishes to seek an exemption under s95 or s95A of the Privacy Act (i.e. for access to, and/or use of, identified personal information, for medical or health research, without the prior consent of the individual) will need to provide prescribed information to enable an ethics committee to consider whether there is a public interest justification for granting such an exemption.

The questions to assist researchers in providing the required information are derived from the guidelines issued under both section 95 and section 95A and the latter include the following:

A.2.6 In the proposal to collect health information for the purpose of research relevant to public health or public safety, the collector(s) should state:

(a) the aims or purpose of the collection;

(b) the credentials and technical competence of the collector(s) of the data;

(c) the data needed;

(d) the study period;

(e) the target population;

(f) the reasons why de-identified information cannot achieve the relevant purpose of the research activity;

(g) the reasons why it is impracticable to seek consent from the individual for the collection of health information;

(h) the estimated time of retention of the health information;

(i) the identity of the custodian(s) of the health information collected;

(j) the security standards to be applied to the health information. Standards must be in accordance with APP1. (Security of Personal Information) (See: Appendix 1)

[Note: In particular, health information should be retained in accordance with the Australian Code for the Responsible Conduct of Research (2018) and in a form that is at least as secure as it was in the sources from which the health information was obtained unless more stringent legislative or contractual provisions apply].

(k) a list of personnel within the collecting organisation or organisations with access to the health information collected;

(l) the level of protection that will be applied by the collector(s) to protect health information disclosed to the collector(s) by the disclosing organisation. These should include:

a) terms of any release agreement between the disclosing organisation and the collector(s) to govern limits on the use and disclosure of collected health information [See: paragraph A.2.9 of these guidelines]; and

b) *proposed methods of disposal of the health information on the completion of the research activity,*

c) *any proposal to send data overseas for the purpose of the research project including the names of the countries to which it is proposed the data be sent and how the research project will comply with APP8 (cross border disclosure of personal information) of the Privacy Act.*

4.1.4 PERMITTED SITUATIONS

The Australian Privacy Principles (APPs) do not apply (so that institutions are not required to comply) if a permitted general situation exists (e.g. "lessening or preventing a serious threat to the life, health or safety of any individual"). The OAIC website lists the permitted general situations and their interpretation. There are also 5 permitted health situations where the APPs do not apply including, where strict criteria are met, health research. See the OAIC website for more about permitted health situations.

4.2 Information Privacy Act 2009

4.2.1 BACKGROUND AND OVERVIEW

In Queensland, the State government first released information standards and then the Information Privacy Act (2009). This Act applies to all Queensland agencies, bodies established under Queensland legislation, and statutory authorities. **As such, the Act applies to Griffith University research.**

The Information Privacy Act applies a modified version of information privacy principles (IPPs) to the above bodies that impose obligations in relation to the collection, use and disclosure of identified personal information. These are discussed in section 4.2.

The Information Privacy Act also applies another set of principles, called the National Information Principles (NPPs) to health agencies, that are defined as Queensland Health or a hospital or health service. They are agencies within the meaning of the Act, and so are entities established by Queensland statute. The NPPs are discussed in section 4.3 below.

Further information about Information Privacy Act and the application of the IPPs in Queensland can be found at the office of the Information Commissioner of Queensland.

4.2.2 THE RESEARCH EXEMPTION

The Information Privacy Act grants exemptions for research and to the compilation of statistics in the public interest, as long as certain criteria are satisfied. The exemptions let a researcher use or disclose personal information, regardless of why it was originally collected, if all of the following apply:

- the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual

- it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
- in the case of disclosure—the organisation reasonably believes that the recipient of the information will not disclose the information.

4.2.3 PUBLIC INTEREST WAIVERS

The Queensland Information Commissioner can give permission for the IPPs or the NPPs to be modified or waived if doing so would be in the public interest. Researchers who are interested in applying for a waiver should contact the office of the Queensland Information Commissioner to discuss the issue.

4.2.4 IMPLICATIONS

The Information Privacy Act applies even if the Griffith University research project is to be conducted in another jurisdiction (including overseas). See Commentary Inset 5 for more on the privacy regulation and research conducted in another jurisdiction.

The Information Privacy Act also applies even if the source of the data is from an entity which is not itself subject to privacy regulation. See Commentary Inset 6 for more on this issue.

Commentary Inset 5 – The Queensland Act and research in other jurisdictions

** research that is conducted in another jurisdiction must still be conducted in accordance with the Information Privacy Act. This is because all of the research conducted under the auspices of the University is subject to the Act.*

If the other jurisdiction has its own privacy regulation it may be necessary for the research to comply with both the Information Privacy Act and the local privacy regulations.

For research conducted within Australia, this is unlikely to be especially problematic as the privacy regulations of the States and Territories are substantially similar to the Commonwealth Privacy Act.

However, for research conducted in other countries there may be some conflict between the Queensland Act and the local regulations. Where this is the case, researchers should contact their local Research Ethics Adviser who will consult with the Office for Research (see contacts) for advice.

The provisions in the Information Privacy Act with regards to accuracy, controlling who can access the data, only using the information for the purposes for which is was collected, and an individual's right to access information about them, all apply to Griffith University research data.

4.3 Information Privacy Act, Health Agencies and the NPPs

> ***Commentary Inset 6 – Statutory privacy issues for bodies that are not otherwise subject to privacy regulations***
>
> *The Information Privacy Act applies only to Queensland government agencies or entities established by an act of Queensland parliament.*
>
> *The Commonwealth Privacy Act applies only to Commonwealth agencies or other bodies (such as non-government organisations with a turnover of more than AUD$3M per year) and also to private organisations that provide health services and have health information.*
>
> *However, Griffith University research that is accessed/collected from a body that is itself not subject to privacy regulation, must still be conducted in accordance with the Information Privacy Act This is because all of the research conducted under the auspices of the University is subject to the Act by virtue of the University having been established/operating by an act of Queensland parliament.*

4.3.1 BACKGROUND AND OVERVIEW

The Information Privacy Act applies a set of health privacy principles (called NPPs, as they were adapted from a set of principles with that name in an earlier version of the Commonwealth Privacy Act) that impose obligations in relation to the collection, use and disclosure of health information held by Queensland government bodies and that provide health services.

4.3.2 RESEARCH EXEMPTION

The Information Privacy Act grants exemptions for research and to the compilation of statistics in the public interest, as long as certain criteria are satisfied. The exemptions let a researcher use or disclose personal information, regardless of why it was originally collected, if all of the following apply:

- if the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or safety
- it is impracticable for the health agency to seek the individual's consent before the use or disclosure; and
- the use or disclosure is in accordance with guidelines issued or approved by the chief executive of the health department for the purposes of this subparagraph; and
- in the case of disclosure, the organisation reasonably believes that the recipient of the health information will not disclose the health information or personal information derived from the health information.

The guidelines referred to can be found here.

4.3.3. PUBLIC INTEREST WAIVERS

The Queensland Information Commissioner can give permission for the IPPs or the NPPs to be modified or waived if doing so would be in the public interest. Researchers who are interested in applying for a waiver should contact the office of the Queensland Information Commissioner to discuss the issue.

4.3.4 IMPLICATIONS

The Information Privacy Act applies even if the Griffith University research project is to be conducted in another jurisdiction (including overseas). See Commentary Inset 5 for more on the privacy regulation and research conducted in another jurisdiction.

The Information Privacy Act also applies even if the source of the data is from an entity which is not itself subject to privacy regulation. See Commentary Inset 6 for more on this issue.
The provisions in the Information Privacy Act with regards to accuracy, controlling who can access the data, only using the information for the purposes for which is was collected, and an individual's right to access information about them, all applies to Griffith University research using health information.

4.3.5 THE QUEENSLAND ACT AND GU OPERATIONAL INFORMATION

Operational data that is collected by the University (e.g. whether a student lives with a disability, or the country of origin of an international student), that is personal information or health information is also subject to the Information Privacy Act. In practice, this means that even if a member of University staff has authorised access to information for operational and/or academic reasons, this does not automatically mean that they have authorised access to that information for research purposes (though the research exemption – see 4.2.2 – may apply).

See Commentary Inset 7 for more on this issue.

Back to contents

5.0 Privacy regulations in other jurisdictions

Most Australian states and territories will have their own statutory privacy framework. Many countries will also have their own privacy regulations. As was noted in 4.2.1 of this Booklet, the Information Privacy Act applies to the use of personal or health information in research. This may also be the case when research is conducted in another jurisdiction. Furthermore, where that jurisdiction has its own privacy regulation the design and conduct of Griffith University research that is conducted in that jurisdiction may need to comply with the jurisdiction's privacy regulations at the research site. In the event that the two statutory instruments are in conflict please contact your local Research Ethics Advisor (who is likely to liaise with the Office for Research) for further advice (see the Contacts section of this Booklet). As a general principle, the higher standard/requirements apply.

Commentary Inset 7 – Privacy regulation and GU student/operational data

GU staff can have access to a range of personal information by virtue of their University appointment (e.g. access to the postal address of graduates, information about students living with a disability, home postal address of University staff). Whilst the staff member will have authorised access to this information for administrative and/or academic purposes, this does not equate to authorised access for research purposes.

For example, a staff member with access to student information about registered disabilities/special needs for the purposes of University service and support delivery, could not access and use this information for research purposes, without complying with the requirements of the Privacy and Data Protection Act or, if the information is health information, the Health Records Act.

In practice, the staff member should approach their access and use of this information for research purposes exactly the same as they would for information held by another body (see 4.2).

5.1 Regulation of international information transfer

There are Australian State and Commonwealth privacy principles and some international regulation that are relevant to the international transfer of any research data from which a person could be reasonably be identified – i.e. personal information.

5.1.1 STATE AND COMMONWEALTH PRIVACY PRINCIPLES

Principles in the Information Privacy Act contain obligations regarding cross-border data flows. In summary, the principles provide that an organisation may transfer personal information to someone outside Queensland if:

(a) the individual agrees to the transfer; or

(b) the transfer is authorised or required under a law; or

(c) the agency is satisfied on reasonable grounds that the transfer is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare; or

(d) 2 or more of the following apply—

(i) the agency reasonably believes that the recipient of the personal information is subject to a law, binding scheme or contract that effectively upholds principles for the fair handling of personal information that are substantially similar to the IPPs or, if the agency is a health agency, the NPPs;

(ii) the transfer is necessary for the performance of the agency's functions in relation to the individual;

(iii) the transfer is for the benefit of the individual but it is not practicable to seek the agreement of the individual, and if it were practicable to seek the agreement of the individual, the individual would be likely to give the agreement;

(iv) the agency has taken reasonable steps to ensure that the personal information it transfers will not be held, used or disclosed by the recipient of the information in a way that is inconsistent with the IPPs or, if the agency is a health agency, the NPPs.

The Commonwealth Privacy Act, on Australian Privacy Principle 8 imposes substantially similar obligations on entities to which the Act applies. The main differences are that such Principle 8 provides that an entity may disclose personal information to a recipient overseas in a number of circumstances that are exceptions to other Australian privacy principles, e.g. the transfer is pursuant to an international agreement for information sharing or is necessary for law enforcement purposes.

5.1.2 INTERNATIONAL REGULATION

The European Union General Data Protection Regulation (the GDPR) that has applied since 25 May 2018, harmonises data protection laws across the EU and replaces existing national data protection rules. In some circumstances, it may apply to Australian businesses.

The GDPR applies to the data processing activities of businesses, regardless of size, that are data processors or controllers with an establishment in the EU. Where a business has 'an establishment' in the EU, activities of the business that involve processing personal data will need to comply with the GDPR, regardless of whether the data is actually processed in the EU.

The GDPR also applies to the data processing activities of processors and controllers outside the EU, regardless of size, where the processing activities are related to:

(a) offering goods or services to individuals in the EU (irrespective of whether a payment is required), or

(b) monitoring the behaviour of individuals in the EU, where that behaviour takes place in the EU (Article 3)

Accordingly, some Australian businesses that are covered by the Australian Privacy Act 1988 (Cth) as APP entities, may need to comply with the GDPR if they have an establishment in the EU (regardless of whether they process personal data in the EU), or do not have an establishment in the EU, but offer goods and services or monitor the behaviour of individuals in the EU.

If your data collection strategy might collect data from EU residents (e.g. you are conducting an open online survey) you will need to add a question to determine if a respondent is an EU resident and then either:

(a) Not collect their information, or

(b) Comply with the GDPR requirements AND the applicable Australian requirements, whether Commonwealth or Victorian.

Contact the Research Ethics & Research Integrity team (see Contacts) for further advice on this matter.

5.1.3 EXPORT CONTROLS

Australia has valid defence, diplomatic and trade interests with regard to the movement of some goods, technology and information overseas. This may be relevant to some of the University's human research projects.

For example, work relating to the genetic modification of a human pathogen may be considered 'dual use research'. These considerations may require special arrangements with regard to data storage and movement, required permits and a modification to how research outputs are reported. This may impact on how data is shared with an international collaborator. Griffith University researchers with questions relating to these matters should contact the Research Ethics & Research Integrity team (see Contacts).

Commentary Inset 8 – Three examples of obligations to disclose

This inset discusses examples for three kinds of situations where a researcher may have an obligation to divulge identified personal information to third parties. These are not intended to be an exhaustive list of the kind of situations where a researcher may have an obligation to disclose identified personal information to a third party.

Professional obligation *– A researcher who is a registered nurse will be observing how undergraduate nurses are supervised while on practicum. Even though the research focus primarily relates to instruction, feedback and debriefing, the researcher will observe some of the care provided to patients. The original intention was not to disclose (or even collect) information about the actual performance of the supervising nurse. It is, however, conceivable that the researcher might observe or become aware of supervising nurses providing inappropriate or unsafe instructions or advice to a student (such as 'shortcuts' to complete medication rounds expeditiously). If this occurs, the researcher would have a professional obligation to intercede and perhaps alert the nursing manager on the ward.*

Legal obligation *– As a component of research that is being funded by a competitive grant, a researcher may be looking at the value of resilience training for early career academics. A component will be reflecting on the family/home challenges that staff members face in addition to their workload and work obligations. It is possible the researchers will be told about domestic violence or child abuse where the researchers might have a legal obligation to notify the appropriate authorities.*

Contractual obligation *– The research grant is funding collaborative research being conducted by Ivory Towers University and a state corrective services agency. This will involve the researchers collecting longitudinal data on prison tertiary education via interviews. Before accessing the agency's custodial facilities, they must sign an agreement indicating they must notify the agency if they are given any information about the smuggling in or distribution of drugs into a facility. Although the topic of the research is unrelated to drug taking, it is likely to place education within the context of life within the facility. If such information were provided, the researchers have a contractual obligation to advise the agency, even though telling offenders that they will pass on information about drugs to the prison authorities might have a chilling effect on prisoners' willingness to disclose other information directly relevant to the research (Palys and Lowman, 2001). Contractual obligations may also affect researchers when researchers obtain information under contract from a third party. This party might be a direct research participant (under a confidentiality agreement or as a consequence of part of a consent agreement), or another researcher or organisation (Chalmers and Israel, 2005).*

6.0 Disclosure of personally identified information

Researchers who have access to/work with identified personal information should not disclose that information to other parties without the consent of the persons named. This includes the way the results of the research are reported or published; sharing identified personal information with other researchers; and the reporting of identified information to third parties.

This is traditionally an application of an obligation of confidentiality that arises as the result of the relationship between researchers and participants and applies to all information provided to researchers by participants, not only identified information. It is an obligation recognised both in law and in ethics. In addition to the legal dimension, the expectation that researchers not divulge identified personal information is also an important ethical responsibility that must be

addressed in the design and conduct of human research under the auspices of an Australian institution. Perhaps one of the most challenging ethical dilemmas is where researchers have a contractual or legal obligation to disclose information irrespective of the view of the persons named.

6.1 Where disclosure may be a professional, legal or contractual obligation or requirement

In some very specific circumstances, human researchers can face a professional, legal or contractual obligation to disclose information (see Commentary Inset 8 for 3 short examples). Such situations are more difficult because this can place the moral responsibility upon the researcher, and requires a reflection upon what action is more ethically justified (e.g. the protection of an assurance of confidentiality, weighed against preventing the spread of an infectious disease). Where such an obligation is predictable this should be discussed in the application for ethics review of the work. As noted at 4.1.4 of this booklet such situations may fall within the scope of a permitted general situation or similar exemption under Queensland legislation (because of a concern for the safety of an individual, or because it relates to a previously undetected crime, or because disclosure is required by law). Researchers who are also members of professional associations (such as the psychologist and nursing bodies) may have a professional obligation to report some matters (e.g. reporting unsafe conduct by another professional). If such an obligation is unexpected and emerges during a project, researchers must promptly notify the Office for Research and seek guidance on how to proceed.
Even trickier is where a researcher feels he or she has a moral obligation to disclose identified personal information (Israel, 2004).

Commentary Inset 9 – Privacy and participatory status

It is important to recognise that third parties knowing the participatory status of individuals can raise significant ethical issues.

This is especially the case where:

i) the data is sensitive;

ii) there are significant risks to participants;

iii) the third party is someone with some degree of power over the participant; and/or

iv) the participants should otherwise be considered vulnerable.

Some reasons why this is the case include:

***Pressure to participate** - Some potential participants (e.g. employees) might feel some pressure to participate in the research if they feel that third parties (e.g. their employer) will know if they have participated.*

***Risks** - In some cases merely a third party (e.g. an abusive family member) knowing that an individual (e.g. the person who has been abused) has participated could create risks.*

Similarly, in some cases a third party (e.g. a peer member) knowing that a potential participant has not participated (perhaps due to them having been screened from the participant pool because they have previously received counselling) could expose those individuals to risk.

***Increased chance of identification** - In some cases significant third parties might be more likely to be able to identify the data that comes from individual participants, if they first know who has participated in the research.*

For many research designs this issue will be moot and/or there really are no significant implications of the participatory status of individuals being known. It is not the case that, for research to be considered ethical, the participatory status of individuals must always be concealed. However, when planning a project, a researcher should consider whether (for the kind of reasons discussed above) there should be measures to conceal the participatory status of individuals.

Furthermore it may be prudent, respectful and perhaps increase the chances of recruiting sufficient participants, if the recruitment and/or consent process discusses the issue of whether others will know the participatory status of individuals.

Further discussion about these matters, specifically with regard to illegal or inappropriate behaviour can be found in Booklet 40 of this Manual..

Back to contents

7.0 Privacy and recruitment

The issues outlined earlier in this Booklet can have significant impact upon the design of the recruitment phase of a human research project. The typical areas of impact are discussed below.

7.1 Identification of persons who are potential participants

A research project can often involve the identification of potential participants from existing files (e.g. persons who have accessed advice with regards to debt management, persons who have been identified as having special needs and have failed a University subject, attendees at a conference about franchising, parents who have sought help with regards to their daughter being bullied at school, users of a particular community domestic violence services who discontinued attendance during the program, or persons who have a particular group of symptoms).

The access to existing files or data to identify persons who meet the selection criteria for a project raises both ethical and statutory privacy issues. Even when a researcher has access to these files for another reason (e.g. a member of academic staff may have authorised access to tutorial lists, attendance records and academic results - but this does not mean they can access those records for research.

At 4.1.1 there is a discussion of the practical implications of the Commonwealth Privacy Act and at 4.1.2.5 there is a discussion about the options/strategies that might be employed.

The GUHREC will try to be flexible in working with the research team to come up with a solution to these matters, but the degree to which the Committee will be able to accommodate alternative strategies will be limited by the provisions of the Commonwealth Privacy Act and the Queensland Information Privacy Act.

7.2 First contact with potential participants

An element of research design, which is often missed in the description of a proposed research project submitted for ethics review, is the initial contact with potential participants. This initial contact can be conducted in many forms, which often can raise ethical as well as statutory privacy issues.

These issues can often be significant because they relate to the rights of individuals, and their potential exposure to risk, possibly prior to them even knowing about the research.

The two most common ethical privacy issues relating to first contact with potential participants are:

1) The degree to which other parties (family members, peers, employer) will know whether the individual is approached about the participation and the degree to which this could then expose those approached to risk (e.g. social, physical, economic and/or legal).

2) The degree to which individual potential participants might consider an approach from a researcher (whether they are known to the individual) about a project/topic to be a form of invasion of their privacy.

A recruitment strategy can involve potential participants being issued with some correspondence about the research project (e.g. seeking their permission for the research team to access their file, a letter inviting them to express an interest in a project, sending them formal recruitment and consent materials, and also in some cases the questionnaire or data collection instrument itself).

Without the prior consent of the individuals concerned, the provisions of the Commonwealth Privacy Act and Queensland Information Privacy Act can, subject to some limited exemptions, make it impossible for personal contact details (e.g. home address, email address) to be disclosed to the researcher at all if the fact that they belong to a potential participant pool is in itself sensitive information. Refer to 4.1.1 and 4.1.2.5 for further guidance on these matters.

Back to contents

Commentary Inset 10 – Internal identification

Internal identification refers to a specific kind of identification by inference. Often when we discuss the question of whether third parties could identify participants (e.g. in the publication/reporting of the results of a research project) we focus upon whether a member of the general public or a typical reader of the published results could identify the participants.

When considering the question of identification, some researchers only consider third party identification by the general public. It is, however, important to consider identification by peers, colleagues, other participants, or people who otherwise know the individual (Tolich, 2004). In many cases, this internal identification by peers may be far more problematic for participants. See Inset Three for an example.

The chance of internal identification becomes more pronounced in case study research and/or where the direct words of individuals will appear. The rich nature of case study descriptions and the peculiarities of some person's phraseology can permit a knowledgeable third party to identify participants, where many other third parties would not be able to identify them.

Such internal identification may not be ethically problematic, and may not be a source of concern for potential participants (e.g. senior officers of a company may not be concerned if they might be identifiable by inference).

However, where such identification is possible the researcher(s) should consider:

i) whether this potential identification could be a source of risk or other concern for the participants;

ii) whether participants should be warned about this potential identification - at the very least assuring potential participants that they will not in any way be identifiable would be inappropriate; and

iii) whether there should be a mechanism where the participants are afforded the opportunity to review their quoted statements or case information to assess whether they wish to see these edited or perhaps to modify or even withdraw their consent.

The possibility for internal identification must be discussed in the application for ethics review (see Booklet 2 of this manual) and in the consent material (see Booklet 22 of this manual).

8.0 Confidentiality

Sometimes the most appropriate and effective way to address the ethical issues relating to privacy (see 3.0 of this Booklet) is by protecting the confidentiality of participants. This is especially the case where the collected information should be characterised as sensitive and/or if disclosure could expose participants to risk.

Depending upon the sensitivity of the collected data/the risks to participants, strategies to protect confidentiality will need to be present in most stages of a research project (e.g. the process of identifying potential participants, recruitment, during data collection, during analysis, in reporting and publication, and in the storage and any subsequent use of the data). The issues to be considered relate to those governed by privacy regimes (see 4.0 of this Booklet) but may also include more general ethical privacy considerations (such as where the data collection will occur and the degree to which participants could be 'overheard').

Generally, confidentiality strategies will relate to the degree to which an individual participant's data (e.g. their comments) can be attributed to individual participants when third parties read the publication or reporting arising from the research. It can also relate to the degree to which third parties can determine the participatory status of individuals (see Commentary Inset 9).

These matters are less of a concern when the collected data is not sensitive/the level of risk is very low.

These matters can be especially problematic when the results of the research will be presented as a case study, retaining the 'voice' of participants, audio or video recordings (see 10.0 of this Booklet), or with sufficient 'richness' of data to enable identification.

It is often useful to distinguish between internal and external identification (see Commentary Inset 10).

As noted in 3.1 because confidentiality arises from the relationship between researcher and participant, preserving the confidentiality of collected data is not an absolute ethical obligation of researchers. Some research participants will very much want their comments attributed to them. Indeed, in some cases individuals will not participate in research unless they will be identifiable and their comments (and contribution to the research) are attributed. In the case of some social media platforms removing the name of the author of a post or in any way modifying the post might be a breach of the platform's rules. This and other privacy matters for online research can be found in Booklet 37 of this Manual.

However, key ethical considerations are the degree to which potential participants understand whether they will be identifiable, whether they have consented to this identification, the degree to which they should be considered a vulnerable group, and whether their identification exposes them to any significant risks.

Data can be initially collected in an identified form, be coded during analysis, then be de-identified in any reporting/publication, and be stored in either a coded or de-identified form.

Commentary Inset 11 – Why is anonymity sometimes necessary?

There will be circumstances where it is preferable for participants to be anonymous, and there are even some cases where the only ethical way to conduct some research is if the participants are anonymous. Some example considerations are:

***Unequal relationship and significant concerns** - Where potential participants are in an unequal relationship (with the researchers or the perceived supporters/sponsors of the research) and there are significant issues/concerns (e.g. there is at least a perceived risk associated with non-participation) then it might be important that no one, not even the researchers, know who has participated in the research.*

***Risks** - Where there is at least a perceived risk associated with the collected data (e.g. disclosures of illegal behaviour) it might be preferable that no one can associate responses with individuals (e.g. even if a law enforcement agency sought access to the data).*

These matters should be discussed and addressed in any application for ethical clearance for a proposed human research project. They should also be appropriately set out in the consent materials that are provided to potential participants in the research.

Back to contents

9.0 Anonymity

Anonymity refers to a situation that exceeds confidentiality (see 8.0 of this Booklet) and refers to situations where the identity of participants is not known.
The decision to the conduct a research project using a form of anonymity will generally reflect the presence of special ethical issues or risks that warrant additional protection for participants (or indeed non-participants). See Commentary Inset 11 for further discussion on this point.

In the case of confidentiality measures, the strategies might only be limited to some parts of the research design (e.g. the data might be collected in an identified form, but it will be reported in a de-identified form). Whereas if participants are anonymous their identity is generally concealed in every element of the research process.

Some sub-sets of anonymity are:

Complete anonymity – a situation where even the researcher(s) will not know which individuals participate and there is no way participants can be identified by inference or data can be directly linked to a participant.

Anonymous responses – a situation where the researcher(s) will know the identity of participants, but cannot link specific data with specific respondents. In some cases, it may be important to ensure that third parties cannot identify who has participated.

Protected anonymity – is a situation where the researcher will know the identity of participants and may be able to link specific data with specific respondents, but will take steps to ensure that third parties cannot link specific data with specific respondents and/or perhaps cannot even determine the participatory status of individuals.

Commentary Inset 12 – Identification by inference

It is generally easy to assess whether participants will be directly identifiable (e.g. because they will be named). However, it is also sometimes possible to identify participants by inference.

This generally occurs where sufficient information about a participant will appear in the reporting of results, such that might enable at least some individuals to infer the identity of individual participants. This can occur with a research design and reporting style, though is most commonly a factor for qualitative research where case study descriptions will appear in the reporting of results/publications.

For example - whilst an individual is not named, to say that a participant is a Brisbane based, research ethics administrator, who has worked in the field for more than fifteen years, and lives with a disability, means that some third parties who read the results of the research will be able to identify the participant.

Such identification may be most likely to be 'internal identification' (see Commentary Inset 10 11) but in some cases this might allow for identification by a wider group.

The fact that identification by inference is possible does not automatically mean that the research is ethically problematic, but it does mean:

1. *The researchers must consider whether this identification by inference means that the research includes a degree of risks to participants or others, and consider whether there is a need for research design features to manage this risk;*
2. *The application for ethical clearance must identify this issue and discuss what, if any, steps are to be taken to address the identification and/or risks;*
3. *The consent, and possibly the recruitment, process will need to discuss these issues so potential participants can make an informed decision as to whether they wish to participate.*

Even though a researcher might believe that a confidentiality strategy, or even a protected anonymity strategy, might afford participants sufficient protection from harm, the researchers are encouraged to reflect upon their ability to protect their participants in the event of receiving a subpoena or other lawful directive to disclose research data. See Booklet 40 of the Manual. In some cases, the only true protection for participants (and sometimes researchers) is for their research data to be of complete anonymity.

The degree to which participation is anonymous can sometimes be an important factor in determining whether an individual will elect to participate in a project. Consequently, it may be important to specifically discuss the situation with regards to anonymity in the recruitment and/or consent materials.

Further information about recruiting participants can be found in Booklet 21 of this Manual. Further information about consent can be found in Booklet 22 of this Manual. The situation with regard to anonymity, and the reasons for the selected approach should be discussed in the application for ethical clearance for the project.

Back to contents

10.0 Identification by inference

Even when individual participants will not be named or directly identified (e.g. in the reporting of the results of the research), it sometimes can still be possible for those participants to be identifiable by inference.
Important considerations for researchers when designing and conducting human research are whether participants will be identifiable:

- through the recruitment and consent process for the research;
- through the collection and analysis of the data;
- through reporting or other research outputs, and
- after the completion of the research.

Identification by inference can occur where sufficient information is present (e.g. in the reported results) that, even though the respondent's name or identity number (see Commentary Inset 12) etc. is not available, it is possible to determine the identity of the individual.

As was noted in 8 of this Booklet, it may be necessary to distinguish between the potential for internal and external identification. In some cases, identification by inference is unavoidable. For example, members of a small work team who are a case study in a research project may well be able to recognise themselves or other members of the team, even when very little demographic information appears in the disseminated results of the research. This can especially be the case where the words of participants will appear in the results because persons who know the participants may be able to recognise them from the quoted phrases.

Despite the fact that individuals might be identifiable, it does not mean that the project is ethically problematic (see 7.0 and 8.0 of this Booklet). Where identification is possible, researchers should reflect upon the degree to which identification may be a source of risk (including social risks such as humiliation) or may otherwise cause concern to the individuals concerned. Where identification by inference is possible (if only by a relatively small group of third parties) it would not be appropriate to describe participation as being anonymous. It should be made clear to the ethics reviewers and potential participants the degree to which identification by inference is possible. Refer to Booklet 9 of this Manual for more about risks.

In cases where identification by inference is possible, one possible strategy (to address any risks and/or the concerns of potential participants) would be for respondents to be offered the opportunity to review the quotes/their stories/descriptions to enable them to check whether they are content with the degree to which they have been de-identified, that they do not feel that they have been misrepresented, and/or to minimise any associated risks to them when the results of the research are published. Inevitably, such a process will need to carefully weigh any impact on the veracity of the results of the research by allowing such editorialising versus the ethical principles of respect and beneficence. Hopefully researcher and participant will be able to negotiate an acceptable compromise. Otherwise, researchers must remember that a

participant should be able to withdraw their consent at any time. Refer to Booklet 43 of this Manual for more about the ethical conduct of case study research.

Back to contents

11.0 Privacy and the re-use of data

There are generally no ethical or legal privacy concerns raised by the reuse of truly de-identified data (e.g. aggregate data where respondents cannot be identified directly or by inference). Nevertheless, it is preferable that the consent that was obtained when the data was originally collected anticipates the possible future reuse of de-identified data for research purposes.

There are also generally no ethical or legal privacy concerns about the reuse of re-identifiable data where the persons who reuse the data are not given access to the data key or other method to enable them to identify respondents. Once again it would be preferable if the consent obtained at the point of the original data collection anticipated the re-use of the data.

Equally, there are no ethical or legal privacy concerns about the reuse of identified data, if the consent of the individuals concerned has been given or is to be sought for that re-use.

Indeed, in the case of the re-use of truly de-identified and re-identifiable data (with the caveat above) such an activity might not be considered to be human research within the scope of the University's human research ethics arrangements (as there are no human participants *per se*, and no use of identified personal information). This is significant for research that will involve access to, and the re-analysis of, data that was collected by another research team or even by another agency, perhaps for quite a different purpose.

The re-use of identified information is likely to require some level of University research ethics review. See Booklet 17 of this Manual for more about the scope and levels of research ethics review at Griffith University. There will be ethical and statutory privacy issues that will need to be considered, specifically with regards to the degree that there will be consent for this access to, and analysis/use of, the identified data.

Another factor in the reflection of whether any re-use of the data is appropriate (even if the data is de-identified) will be the nature of the assurances provided to participants in the original research about how their data would be treated (e.g. were they told that their data would not be used for any additional purpose?). A typical assurance about confidentiality is unlikely to prevent the re-use of de-identified information. But such an assurance might mean that there will need to be serious reflection about the reuse of re-identifiable information. Furthermore, it would not be possible to re-use identified data unless specific consent was sought for this reuse.

Commentary Inset 13 – Re-identifiable data

Re-identifiable data (otherwise known as coded data) refers to data that are stored (and sometimes analysed) in a form where the identifying information has been removed and replaced with a code. The research team will possess a code key or other mechanism to enable them to re-identify entries. In most cases this code key will be stored separately, and at some point (e.g. once data analysis is complete), the code key will be destroyed. At that point the data are truly de-identified and not even the researchers will be able to link data to individual participants.

If data are provided to researchers in a coded form, but the research team is not provided with the code key, this is for all intents and purposes de-identified data.

Sometimes, researchers will possess other data that, with cross matching, could enable the identification of data that might otherwise appear to have been de-identified.

You can find more information about research involving the re-use of previously collected data in Booklet 42 of this Manual.

Back to contents

12.0 Sharing data with other researchers

Related to the reuse of data (see 11.0**) is the sharing of data with other researchers. The first consideration is whether the data are identified/identifiable by the researcher who will receive the data. If the data are identified, they can only be shared with the consent of the participants (whether in the form of a specific consent or more generally for the sharing of identified information with other researchers).**

Even when the data are de-identified, the researcher should consider the following matters:

i) are the data highly sensitive so the sharing of data in anything but an aggregate form may be a concern for some participants?; and/or

j) did the original consent specifically exclude the sharing of data in any form?

Back to contents

13.0 Privacy and the storage of data

The storage of research data can raise a number of significant ethical issues. Important questions include where the data will be stored, how secure is the data, is access to the data controlled, and how long will the data be retained?
It is also important to bear in mind that the storage of identified (or even re-identifiable) information is subject to the provisions of the APPs, IPPs and NPPs (see 4.0 of this Booklet) articulated by the Commonwealth and Queensland privacy regimes.

13.1 Location

13.1.1 Security

A key consideration with regards to the location for the storage of data is the degree to which the location is secure and appropriate. This issue is most significant when the data are to be stored in an identified or re-identifiable (see Commentary Inset 13) form. It becomes vital when there is some form of risk if third parties were to see the identified data.

13.1.2 During the research

Depending upon the nature of the research and practicalities, the data may be stored in a temporary or 'working' location that is different from the post-research location (see Section 13.1.3 of this Booklet). Nevertheless, the same principles in terms of security still apply. The need for security also applies with regards to the transport of data (e.g. when a researcher is travelling between sites and will have data in the possession during the travel).

13.1.3 After the research

As per the requirements of the Australian Code for the Responsible Conduct of Research (2018), the University has produced the GU Framework for the Responsible Conduct of Research. The GU Code includes a *Schedule of Retention Periods for Research Data and Primary Materials*. This schedule articulates the minimum timeframe during which research data (and other relevant materials) must be retained. Generally, at least a copy of the data should be retained under the control of the University for this time period.

Commentary Inset 14 – Consent for other use of data

In addition to the research analysis of audio or video recordings, work samples, or other data, a researcher may also want to use the data for another purpose (e.g. play an excerpt during a conference presentation to illustrate a point).

It is important to realise that, even though the participant won't be named, depending on the nature of the data and what will be shared, it is possible that third parties will be able to identify a participant.

Both ethical and legal principles require that consent be sought for such a use.

Some potential participants, who might be willing to participate in the research, will not be willing to have the potentially identifiable data about them used for the wider purpose.

For this reason, it is often advisable to separate the consent for the wider use from the consent for the research.

Typically, this is achieved through a tick box which enables the participant to opt out of the wider use/presentation of the audio visual, work sample or other data about them.

Ideally the consent material should explain what they should do if they wish to later withdraw their consent for the wider use of the materials. Sometimes this can be a cultural issue, but there may also be legal or other reasons for a participant to wish to later withdraw their consent.

Even though consent may have been obtained, the researcher(s) must continue to observe the ethical principle of respect for persons,and ensure that the uses of the material are consistent with the consent obtained, and do not expose individuals to additional risks.

In cases where significant sensitivities exist it might benecessary to further preserve the anonymity of individuals (e.g. by pixelating their face, disguising their voice, or other similar precautions).

13.2 Access

13.2.1 Research team access

Important ethical, and indeed in some cases statutory, considerations are:

a. who will have access to the data and the form of the data that will be accessed (identified, coded/re-identifiable, or de-identified).

b. if the data are coded, will the code key be stored in a separate location, and who will have access to the code key?

c. will there be controls on who can access the data?

d. will the data be located in a secure location and will there be administered, supervised and/or logged access?

In the case of genuinely de-identified data (where all personal identifiers have been removed and there isn't a mechanism to re-identify the data), or data without significant risks, there would not normally need to be much in the way of access controls. However, in the case of sensitive data and/or data with associated significant risks, especially when the data will be identifiable by the person accessing the data, there would normally need to be a number of access controls.

Depending on the sensitivity of the information collected, these matters must be addressed in the research design, discussed in the ethics application and appropriately explained in the consent materials.

13.2.2 Third party access

Will third parties be authorised to access the research data? In what form will this access take (identified, coded/re-identifiable, de-identified)? Will third parties have access to an identifying code key?

Will there be administered, supervised and/or logged access? Will there be arrangements to safeguard against unauthorised third party access?

Depending on the sensitivity of the information collected, these matters must be addressed in the research design, discussed in the ethics application and appropriately explained in the consent materials.

13.3 Retention period

The University has produced the GU Framework as our implementation of the Australian Code. The GU Code includes a disposal schedule. This articulates the minimum timeframe during which research data (and other relevant materials) must be retained.
In some cases, a research team may wish to retain data beyond this minimum period for additional analysis and use (e.g. in conference presentations). Even if these data will be stored in a de-identified form (see 8.0) the consent obtained when the data are originally collected should ideally anticipate this retention and future reuse (see 11.0). At the very least, to make such a retention for reuse defensible, future uses of the data should not be precluded by the original consent (e.g. with a statement such as "Your information will only be used for this research project"). Where the data will be retained in an identified form or includes audio visual material specific consent must be obtained for the retention. It may also be appropriate to enable participants to separately express their consent for this retention (see Commentary Inset 14) and to perhaps later reconfirm consent for the specific reuse (see Commentary Inset 15).

Commentary Inset 15 – Reconfirming consent for the re-use of data

Further possible uses for data can arise after the participants in the research have given their consent. Indeed, sometimes such opportunities can arise after the research is completed.

When the reuse will involve de-identifiable data, it may not be necessary to either consult with the participants or the Office of Research Ethics and Integrity. However, where the reuse will involve working with identified data or the publication of pictures, audio-visual media or work samples, and if the original consent did not anticipate this use, it may be necessary to seek additional consent.

Sometimes, even though consent that anticipates the re-use was obtained, where there a risks or significant ethical sensitivities, it may be appropriate to confirm the consent for the reuse of the data.

When such a reuse emerges, the researcher(s) should contact their local Research Ethics Adviser, who may consult the Office for Research (see contacts).

The University's eResearch Team manage a data storage mechanism specifically designed to meet the requirements outlined by 13.1 and 13.3 of this booklet. It is appropriate for sensitive data and allows for sharing with researchers outside of the University. The use of this service is not compulsory but is highly recommended.

13.4 Disposal

At the end of the mandated retention period (see 13.3) the data and materials should be destroyed, unless there is valid consent for the retention of the data for additional uses.

In the case of sensitive data and materials, especially when they exist in an identified form, there may need to be security precautions with regards to the destruction of the data and materials (e.g. using a recognised secure document destruction company). In other cases, it may be sufficient to merely shred and then dispose of the data.

When planning a research project, the researcher(s) will need to consider, and possibly make arrangements for, the appropriate disposal of the data. This plan may need to be modified if the details and circumstances of the research change (e.g. if the collected data proves more sensitive than the researcher(s) had originally thought). In the case of highly sensitive data, it may be a matter of reassurance to potential participants to be told of the planned approach to the disposal of the data.

Please note that, in addition to the research retention provisions in both the Australian and University responsible conduct of research codes, research that is conducted under the auspices of Griffith University is also subject to the Public Records Act, as such, the time frames for, and the manner of, the disposal of research data and materials are subject to statutory control.

Back to contents

Commentary Inset 16 – Example of the separation of administrative information from research data

Survey of industry partners *– Contacts at businesses that have hosted undergraduate students will be asked for their perceptions of the preparedness of the students they have been sent by University of the Western Suburbs and the support the host received from the university's practicum office. The researchers decided to conduct this web survey anonymously to maximise the candour of the respondents, but also decided to increase participation rates by entering respondents into a prize draw to win a music voucher. To resolve the problem of both conducting the survey anonymously and entering the respondents into the prize draw the researchers will:*

- *Store the survey data in a separate unmatched table from the prize draw entry information (i.e. there is no link between the two).*
- *Provide visual clues that the survey question and prize draw entry questions are completely separate.*
- *Have a staff member not involved in the practicum placements 'open' the prize draw entries, conduct the prize draw and then securely erase the prize draw entries.*
- *Explain these arrangements in the recruitment and consent materials and when reporting the results of the research.*

Similar arrangements could be employed for offline data collection and for other administrative information.

Any such arrangements should be discussed in the application for ethics review.

14.0 Consent

Appropriate discussion on the matters covered by this booklet should be included in the consent materials that are provided to potential participants (including data storage).

Where there are issues of particular concern, because a privacy issue raises a legal or ethical concern or a potential harm to participants, the GUHREC will expect to see that matters discussed in appropriate detail in the consent materials.

The provision of this information to potential participants not only ensures that they can give consent with regards to this element of the research, but experience suggests that where there are some doubts as to how their privacy will be handled, many individuals will elect not to participate in research that they might otherwise have been willing to be involved in.

This is one of the reasons why it is important that the research ethics reviewers of proposed work can review the consent materials at the same time as the application for ethical clearance. See Booklet 22 of this Manual for more about consent.

Advice with regard to some common situations for University research are discussed below.

14.1 Separation of information to administer the project from research data

In some cases, researchers might decide to collect data without attaching personal identifiers. There can, however, be the need to register that an individual has participated (e.g. to enter them into the prize draw incentive). One solution to these two apparently incompatible objectives is to collect and store separately the research and administrative data. Commentary Inset 16 discusses one example of such an approach. It is important that both the application for ethics review and the consent mechanism (see Booklet 22 of this manual) explain that despite the administrative information that is collected, the researchers will not be able to associate responses with individuals and that the administrative information is stored in a separate and unmatched table. In some cases, it may be desirable to have another party process the administrative data so the researchers remain unaware of the participatory status of individuals. Once again, this should be explained through the recruitment and consent mechanisms.

Commentary Inset 17 – Example of the Opt-out approach and the use of course evaluations

A Deputy Head of School (Academic) wants to analyse course evaluations over a ten-year period. He is interested in whether differences in student satisfaction can be correlated to the method of delivery rather than teaching staff. Even though such an evaluation is (at least arguably) within the scope of the Deputy's official review he wants to use the collected information and some exemplar student comments in at least one research paper.

Most of the research analysis will be on data aggregated over the ten-year period. Course delivery method will be reported but neither the title of the unit nor the year. Because of the volume of information, he contends identification by inference or internal identification is highly improbable and there is no more than a low risk of harm to the student.

Despite this, the Deputy is conscious that teaching staff might be internally identifiable by their colleagues. Consequently, the Deputy will seek express consent from the teaching staff, which will outline the measures to reduce the likelihood of identification and will explain how he believes the benefits justify the risks.

He will be seeking ethical clearance for the opt-out approach for access to student records because:

- *the volume of students (many of whom the School no longer has current contact details for) make it impractical to seek express consent from them*
- *the information that will be accessed and used is not sensitive and the use of an opt-out approach is not precluded by State, Commonwealth or International law*
- *it is vital that the dataset be as close as possible to complete*
- *the potential benefit of improving the effectiveness of the school's educational strategies offers a tangible improvement for students and financial value that far outweighs the limited impact upon the privacy of the students.*

A notice about the research, of de-identified student comments and course evaluations will be publicised:

- *in alumni and school newsletters (that are sent to agencies where many of the school's graduates work)*
- *on the school's website and social media presence*
- *in a broadcast email that will be sent to the last contact details the school has for the students.*

The above material will indicate that students have 90 days to contact the school's administration officer to indicate they don't want their information used for the project. The SAO will maintain a secure register that records if individuals have been in contact and their views. The SAO will provide to the Deputy only the information of the students who have not indicated they didn't want their information used.

Rather than the opt-out approach, the Deputy could have sought a waiver of the consent requirement. However, the Deputy felt that it would be more respectful to publicise the research and give the students the opportunity to opt-out.

14.2 The recording of 'participants' without consent

As discussed at 3.0, as a general principle prior consent must be obtained for the collection/access to personal information/data. That consent can be specified, extended or unspecified. At 4.1.2.3 there is discussion of the waiver of consent mechanism.

It is unlikely that an Australian ethics review body would grant clearance to a project where individuals are to be photographed without consent

especially where the identification of individuals by third parties was a possibility (even if this identification would 'only' be by peers and colleagues – identification by inference as discussed at 10.0).

The *Harvard Researchers Used Secret Cameras to Study Attendance. Was That Unethical?* case (*Chronicle of Higher Education*, 2014) raises an interesting issue with regard to the photographing of students without their prior consent. Commentary Inset 18 reflects upon how the imagery could have been collected in a manner more likely to receive ethical clearance from an Australian ethics review body. Of course, such a research ethics review body might still require the researchers obtain a waiver of the consent requirement (see 4.1.2.3).

See Booklet 2 of this Manual for more about ethics review and see Booklet 22 of this manual for more about consent mechanisms.

14.3 Access to GU historical records

Throughout their normal operations, institutions collect/generate a large volume of information of potential interest to researchers. These data sets can include teaching and course evaluations, records of student academic performance, practicum reports, disciplinary proceedings and other operational matters of potential research interest. The information in these records might be current, recent or historical in nature, potentially relating to periods of many decades. The records are likely to include personal information, but the information is unlikely to fall within the categories the Commonwealth Privacy Act or the Queensland Information Protection Act stipulate are sensitive. Legally a researcher cannot access the information in an identified form, and consent of those whose records are being accessed is not practical. The opt-out approach may be an option for some projects. This option is discussed at 14.5 of this booklet and an example of the use of the opt-out approach is discussed in Commentary Inset 17.

14.4 Work products

Student assignments and other work products can be a valuable source of data for research and can provide illustrative examples for reports, conference papers, articles and other research outputs. They cannot, however, be used for research purposes (even if personal identifiers are removed) without the consent of the authors (so the use of the samples should also be approached like personal data). The use of the sample should also be approached just like any other piece of academic work with the same authorship protections as other academic publications (see the authorship provisions in the *Australian Code for the Responsible Conduct of Research*, NHMRC & ARC 2018).

Commentary Inset 18 – The ethical collection of photographic information without consent

The Chronicle of Higher Education (November 2014) reported a story about Harvard University researchers using hidden cameras to track the usage of seats in 10 classrooms. Even though there is some dispute about whether the work was in fact research, the article poses the question of whether the work was ethical.

It is perhaps useful to reflect upon whether a similar design could be used for human research in Australia.

Employing low resolution *– One possible approach could have been to intentionally set the resolution of the cameras so low that while it would be possible to determine whether the space was in use, the identification of individuals would be impossible. Alternatively, if only the faces of individuals were pixelated there would be a period of time where the researchers might know the identity of individuals. Furthermore, if the images were published the students might still be identifiable by their peers.*

Researchers should consider the following issues before using a student's work for research purposes. They ought to:

- Obtain consent for the research use of the work product as per Booklet 22 of this manual. The information provided to the student should explain the ways in which the paper will be used and who is likely to have access to their work.
- Ensure that students understand their decision will have no bearing upon the grade they will receive for the work. Ideally consent should be sought for the research use of the work product after marks for the assessment have been returned – or perhaps even after the results for the semester have been issued (Takacs, 2002).
- Consider the degree to which the people who are likely to view the work may be able to identify the student (by identification by inference). These factors may be a source of embarrassment or even humiliation for the student, especially if the work is going to be used as an example of incorrect technique or poor performance (Linkon, 2002).

14.5 The 'opt-out approach'

The opt-out approach is an addition to Chapter 2.3 of the National Statement. Rather than a form of consent, it is perhaps more accurately described as a recruitment strategy where individuals, in response to a request, contact the researchers if they don't want their information used for a research project.

The opt-out approach **can only** be used where:

- The public interest in the proposed activity substantially outweighs the public interest in the protection of privacy.
- It is justifiable and reasonable to assert that the research activity is likely to be compromised if the participation rate is not near complete, and the requirement for explicit consent would compromise the necessary level of participation.
- The use of the opt-out approach (rather than express consent or a waiver of the consent requirement) is not legally precluded.
- The research involves no more than a low risk of harm.

A valid opt-out mechanism will:

- make reasonable attempts to provide all prospective participants with appropriate, plain language information explaining the nature of the information to be collected, the purpose of collecting it, and the procedure to decline participation or withdraw from the research
- provide a reasonable time period between the provision of information to prospective participants and the use of their data so that an opportunity for them to decline to participate is available before the research begins
- provide a mechanism for prospective participants to obtain further information and decline to participate
- manage and maintain the data responsibly in accordance with relevant security standards (see 16.0)

- have a governance process in place that delineates specific responsibility for the project and for the appropriate management of the data.

See Commentary Inset 17 for an example of a valid use of the opt-out approach in a project involving the research use of course evaluations.

One of the advantages of the opt-out approach (if it complies with the two sets of points above), compared to a waiver of the consent requirement, is that there will be an attempt to reach potential participants and invite them to express their wishes. Conversely, a waiver is considered and approved just by a research ethics committee with no advice to potential participants.

However, there are some further requirements for using an opt-out approach for consent to the use of personal information to which the Commonwealth Privacy Act applies. These are contained in paragraph B40 at page 10 of guidelines on the Australian Privacy Principles.

See 18.0 of Booklet 21 of this manual for more about the opt-out approach.

14.6 Reconfirming consent

There can be circumstances (see the list below) where a researcher may need to reconfirm the consent of the relevant participants before releasing the output (e.g. report or journal article) from the research.

The two most obvious circumstances where it may be necessary to reconfirm consent are:

- before including attributed quotes or otherwise identified data
- to check that the individual is comfortable with whether and how they have been de-identified.

A new consent mechanism will probably be necessary where there is to be a new kind of output (e.g. originally the consent referred to a report to the funding body but it is now intended to produce a journal article) especially if there is a heightened possibility that individuals will be identifiable.

14.7 Withdrawal of consent

As per NS 2.2.20, except where any limitations are explained to potential participants, they must be able to withdraw their consent at any point. The *National Statement* does recognise that it may be impossible for this withdrawal to also allow the removal of the participant's data from the research. For example, if participants are completing an anonymous survey or if the data will at some point have the personal identifiers removed it would be impossible for the researchers to delete an individual's data after the survey is completed or after the point where the personal identifiers have been excised. The practical implications of NS 2.2.20 are:

- Participation in research must be voluntary and a component of this is the right to withdraw consent.
- If there are any practical limitations to removal of the data, these must be explained to potential participants.

Back to contents

15.0 Recruitment materials

In addition to the information included in the consent materials (see 14.0), it is sometimes necessary (or at least a prudent reassurance for potential participants) to discuss privacy issues in the recruitment materials (e.g. the flyer calling for volunteers who are interested in participating in the research).

The National Statement 2018 specifies that all recruitment materials (e.g. letters, notices, advertisements) must be approved by the ethics review body prior to their use. Preferably these should be as an attachment to the application for ethical clearance, or they may be submitted to the Office for Research later for review.

Back to contents

16.0 Research integrity matters

As was noted at 13.0, in addition to the ethical considerations, privacy matters in human research also have a research integrity dimension. In addition to the Griffith University Framework, the University's research integrity page includes a number of resources for researchers (e.g. additional guidance with regards to the responsible management of research data).

Matters to be considered are:

1) the security of the information during the project and how access to the information will be controlled
2) who will have authorised access to the information
3) if the information will be moved or communicated between locations, how this will be done securely
4) if the data will be coded, who will have access to the code key and will the code key be erased at some point
5) how the data will be stored for the requisite period after the completion of the project (as per the *Australian Code for the Responsible Conduct of Research and the University's requirements*.)
6) if there are any reasons for the retention of the information beyond the requisite period (e.g. because of its potential historical or cultural significance)
7) whether the data/information will be made available for future research use and if this will be in an identified or de-identifiable form
8) how the data/information will be destroyed securely
9) the appropriate description of these matters in the consent materials (see Booklet 4 of this manual).

Back to contents

17.0 Responsibilities of researchers

As discussed previously, researchers have important ethical and regulatory responsibilities in designing, conducting and reporting human research. These responsibilities apply to all human research irrespective of the design, discipline, level or funding source.

In summary, these responsibilities are to:

- only collect, access and use identified personal information that is necessary for the research
- obtain consent or waiver of the consent requirement for collection, access and use of personal information
- handle identified information responsibly (including safeguarding against unauthorised access to the information)
- not disclose personal information to third parties without prior consent or ethical authorisation (see Contacts)
- when reporting the results of research or producing outputs of the research, not disclosing the identity of individuals without prior consent or authorisation from the ethics review process (see Contacts).

Back to contents

18.0 Research ethics review

Applicants need to outline how the design and conduct of a project will address the matters discussed earlier in this section (especially the numbered points at 16.0). Failure to do so is likely to cause delays to the ethics review and authorisation to commence the research. If the omissions are serious and are likely to expose participants to risks from identification (e.g. because the information/data are personally identified and deal with matters that are sensitive), ethics reviewers may return the application for revision and resubmission.
See Booklet 2 of this manual for more about ethics review.

Back to contents

19.0 References and other recommended reading

Allen AL 1997, 'Genetic privacy: Emerging concepts and values', in Rothstein MA (ed.) *Genetic Secrets: Protecting privacy and confidentiality in the genetic era*, Yale University Press, New Haven, pp. 31–60.

Beauchamp TL & Childress JF 2001, *Principles of Biomedical Ethics* (5th edition), Oxford University Press, New York.

Chalmers, R & Israel, M 2005, *Caring for Data: Law, professional codes and the negotiation of confidentiality in Australian criminological research*, Report for the Criminology Research Council. Available at: http://www.criminologyresearchcouncil.gov.au/reports/200304–09.html (Viewed 21 June 2015).

Chronicle of Higher Education 2014, 'Harvard researchers used secret cameras to study attendance. Was that unethical?'. Available at: http://chronicle.com/article/Harvard-Researchers-Used/149865/ (Viewed 6 November 2014).

Israel, M 2004, 'Strictly confidential? Integrity and the disclosure of criminological and socio-legal research', *British Journal of Criminology* vol. 44, no. 5, pp. 715–40.

Israel. M 2011, *The key to the door? Teaching awards in Australian higher education*, Australian Learning and Teaching Council, Sydney. Available at: http://www.olt.gov.au/system/files/resources/Israel%2C%20M%20UWA%20Fellowship%20report%202011_0.pdf (Viewed 21 June 2015).

Privacy Act 1988 (Commonwealth). Retrieved from https://www.oaic.gov.au/privacy-law/privacy-act/

Kaiser, K 2009, 'Protecting respondent confidentiality in qualitative research', *Qualitative Health Research,* vol. 19, no. 11, pp. 1632–1641.

Linkon, S 2002, 'Going public with students' work: The movie', in Hutchings, P (ed.), *Ethics of Inquiry: Issues in the scholarship of teaching and learning*, The Carnegie Foundation for the Advancement of Teaching, Menlo Park, CA, pp. 75–77.

Takacs, D 2002, 'Using students' work as evidence', in Hutchings, P (ed.), *Ethics of nquiry: Issues in the scholarship of teaching and learning*, The Carnegie Foundation for the Advancement of Teaching, Menlo Park, CA, pp. 27–34.

NHMRC 2018a, National Statement on Ethical Conduct in Human Research (2007 updated 2018). Available at https://nhmrc.gov.au/about-us/publications/national-statement-ethical-conduct-human-research-2007-updated-2018 (Viewed 12 October 2019)

NHMRC 2018b Australian Code for the Responsible Conduct of Research. Available at https://www.nhmrc.gov.au/about-us/publications/australian-code-responsible-conduct-research-2018 (Viewed 12 October 2019).

NHMRC (2019) Management of Data and Information in Research. Available at https://www.nhmrc.gov.au/file/14359/download?token=0FwepbdZ (Viewed 12 October 2019).

Palys, T & Lowman, J 2001, 'Social research with eyes wide shut: The limited confidentiality dilemma', *Canadian Journal of Criminology,* vol. 43, no. 2, pp. 255–267.

Stiles PG, Boothroyd RA, Robst J & Ray JV 2011, 'Ethically using administrative data in research: Medicaid administrators' current practices and best practice recommendations', *Administration & Society,* vol. 43, no. 2, pp. 171–192.

Tolich M 2004, 'Internal confidentiality: When confidentiality assurances fail relational informants', *Qualitative Sociology,* vol. 27, no. 1, pp. 101–106.

Back to contents

Acknowledgements

Some amendments to this booklet (from the version 3.6 to 3.7 drew upon a resource booklet commissioned by the Australian Government Office for Learning and Teaching, and produced by Prof. Colin Thomson, Dr Gary Allen and Prof. Mark Israel (Australasian Human Research Ethics Consultancy Services).

Back to contents

Contacts

There are a number of resources available to assist researchers formulate an appropriate response to a question or challenge about the design and/or conduct of a project. This includes the Griffith University Research Ethics Manual and the Human Research Ethics Information Sheet Series. These documents are available from the URL below.

Research students – The first point of contact for research students for advice on any research ethics matter is always your supervisors.

REAs – All academic elements of the University have been asked to appoint at least one member of academic staff as a Research Ethics Advisor. REAs are a local contact for advice, information and suggestions. The contact details of all the current REAs can be found on the URL below.

Office for Research – Staff in the Office for Research (see below) are available to advise with the process of lodging an application or other administrative matters, procedural or policy questions. However, you will be asked what advice you have sought or received already (e.g. consultation with the REA for your area).

Manager, Research Ethics and Integrity

Tel: (07) 373 54375
research-ethics@griffith.edu.au

Policy Officer, Research Ethics and Integrity

Tel: (07) 373 58043

Research Ethics Systems and Support Officer

Tel: (07) 373 5 2069

On the ethics web site you will find:

https://www.griffith.edu.au/research/research-services/research-ethics-integrity/human

- The other booklets of the *Griffith University Research Ethics Manual*
- The *Griffith University Human Research Ethics Information Sheet Series*
- Either downloadable copies of, or links to, the various application forms
- Contact information for the Research Ethics Advisers (REA) and other contacts
- Educational and other resource material
- Useful external links

Griffith University is commercialising the GUREM through licenses to other universities and research institutions. Consequently, Griffith University staff are asked not to send copies of any booklet to persons external to Griffith. For further information please contact the Office for Research (see above).