Research Ethics

Human Research Ethics Committee (HREC)

Guideline:
Harm and Risk in Research

Introduction

Research involving human participants must have a benefit to society and the risks involved to participants must be balanced against the potential benefit to the overall community. The researcher must describe the magnitude and probability of foreseeable risks or discomforts that the subject may experience, including harm, deception, privacy and confidentiality. Invasive procedures always involve some uncertainty regarding harmful effects, thus, risks should be explained in terms of the probability of their occurrence. The researcher needs to be aware of the fact that individual perception of the nature of risk varies and she or he may need to determine whether a participant is one who is a risk taker, ignores the risk(s) or has not properly understood the probability of the risk(s). If prospective participants enquire about risks or other aspects of the research, the investigator must supply an explanation.

Definitions

Harm: means an injury to the rights, safety or welfare of a research participant that may include physical, psychological, social, financial or economic factors. It is responsibility of the researcher to avoid, prevent, or minimize harm to others.

- **Physical Harm:** Actions or situations may cause bodily harm, in which participants may experience injury or death.
- **Psychological Harm:** Deception or mishandling of information may result in mental or emotional trauma for the participants.
- **Social Harm:** Detailed use of information may be hazardous to the social position of an individual or may be detrimental to groups of people in the participant's community.

- **Financial/Economic Harm:** Loss of privacy may result in a loss of benefits, insurance, or employment for the participant.
- **Harm to Participants' Rights:** Failure to complete the informed consent process or to respect subjects' autonomy could contravene participants' rights. See the Guideline on Informed Consent (HRECG2)

The principle of minimising harm implies that research will involve the least number of human subjects and the fewest number of tests on these participants required to ensure that data is scientifically valid.

Risk: pertains to the possibility of harm in terms of magnitude, probability, and permanency. In general, research should not involve more than minimal risk (the threat of magnitude and probability of anticipated harm is not greater than that experienced in everyday life or during routine physical or psychological tests or examinations). In research involving more than minimal risk, the participation of human subjects must be crucial to the achievement of important scientific or societal aims that cannot be accomplished in any other way. All reasonably foreseeable risks should be explained in the process of informed consent.

- ***Potential Risks of the Research:*** The researcher must describe the magnitude and probability of foreseeable risks or discomforts the subject may experience including common risks (inconvenience), soft risks (embarrassment, limitations on confidentiality) and potentially serious risks (adverse effects), indicating the likelihood of such occurrence. Invasive procedures always involve some uncertainty regarding harmful effects, thus, risks should be explained in terms of the probability of their occurrence.

Deception: In general, research involving deception, concealment or covert observation is not considered ethical because voluntary and fully informed consent cannot be obtained.

Exceptional circumstances in some fields of research, such as the study of human behaviour, may require deception, concealment and covert observation.

The Research Ethics Committee may consider research involving deception, concealment or covert observation, if specific requirements are met, for example, if:

- the scientific validity of the outcome of the research would be jeopardised if participants were provided with information regarding the objectives, procedures and methods of the research;
- the extent of such activities is specifically defined;
- the desired information cannot be acquired through alternative methods;
- the participants do not experience increased risk due to such activities;
- the disclosure to the participants is adequate and prompt and de-briefing of each subject occurs as soon as possible after participation is completed;
- the participants are allowed to withdraw data which they provided without their knowledge or consent during the research process;
- such activities will not have a negative effect on the relationship between researchers/research and the community;
- the participant should re-consent to the use of the data obtained by deception once the debriefing process is completed.

In the event that deception is unavoidable a debriefing for research participants is necessary following such studies. The researcher should clarify for the participants the real nature of and rationale for the research and seek to remove any misconceptions.

Privacy: Individuals have a right to keep a part of their lives free from intrusion, and information privacy is an area of particular importance. A fundamental requirement of ethical research is that information disclosed within the context of a research relationship be kept

confidential. The researcher has a duty not to share confidential information with others, without the participant's voluntary, informed consent. However, confidentiality is not absolute, sometimes research values and societal values conflict, in which case, the infringement of privacy and confidentiality may be justified in regard to public interests. due to legal requirements or where other principles may take precedence over privacy as required by law. For example child protection legislation as outlined in *Children First* (1999) considers the limits of confidentiality where an adult is concerned that a child (either the participant or someone they refer to) is a risk of harm or abuse.

Confidentiality: It is the duty of the researcher to protect the level of confidentiality agreed in the informed consent process, as far as is legally possible. Research participants must be informed of the extent to which confidentiality can be maintained and the measures taken to ensure this level of confidentiality. This is particularly important when conducting research with children in situations where complete confidentiality cannot be guaranteed (e.g. when collecting identifiable data). Anonymity is the best protection of confidentiality in regard to personal information and records. However researchers should be aware that the public nature of focus group methodology means that neither anonymity nor confidentiality can be guaranteed as the actions of the group members are beyond the direct control of the researcher.

Personal Data for Research: when data relating to a living individual who can/ may be identified either from the data or partially from the data together with other information comes into the possession of the data controller (the researcher or legal person), they are responsible for the use and retention of the data. Researchers must ensure that they manage the collection and storage of personal data from participants in accordance with GDPR and Data Protection legislation. It is the researcher's duty to collect the minimum personal data

necessary for the research and to store it wiht the appropriate level of security compliant with GDPR requirements to protect participants.[1]

Personal Sensitive Data: collectd by researchers constitutes a high level of risk to particiapnts shoudl it be made public. It is the researcher's duty to collect only the minimum, necessary personal sensitive data, and to protect the participant by storing it at the highest level of security compliant with GDPR. Personal sensitive Data can be found in the following:

- medical records of patients,
- employment (HR) records,
- criminal records,
- immigration records,
- social security and welfare records,
- details of membersips of a trade union etc.

Personal Information: may be classified into one of four types of data: anonymous; identified; potentially identifiable; and de-identified.

- ***Anonymous data:*** is information collection without any identifiable personal information (identifiers) such as anonymous surveys and questionaires;
- ***Identified data:*** refers to information which has identifiers attached to it, meaning that specific individuals could be identified. Identifiers include factors such as the individual's name, address, city, county, postal code, elements of dates directly related to an individual (such as dates of birth, death, admission, discharge, etc.), phone and fax numbers, electronic mail addresses, account numbers, certificate/license numbers, vehicle and/or device identifiers and serial numbers, web universal locators (URLs), internet protocol (IP) address numbers, biometric identifiers including finger and voice

[1] For more information on personal data see http://www.ucd.ie/gdpr/about/personaldata/

prints, full face photographic or comparable images, and unique identifying numbers (not codes assigned to data by researchers).

- ***Potentially identifiable data:*** is coded information that can be re-identified. Coded means that the identifiers have been removed and replaced by a symbol, such as a number, a series of letters, another name, etc. This is a reversible process of de-identification in which it is possible to use to the code to re-identify specific individuals related to the data. Within qualitative research it is important to remember that recordings of interviews or focus groups can be considered potentially identifiable, even if audio tapes or audio files have no identifiable markings on them. In addition, transcribed qualitative data which has not been thoroughly de-identified can also be considered potentially identifiable data.
- ***De-identified data:*** refers to information that has been rendered anonymous, thus not re-identifiable. The data has either never been identified or the identifiers have been permanently removed. For example, transcripts of an audio recording, which do not bear any reference to identity of the person featured in the recording, or medical records wiht all identifiers removed. De-identification is an irreversible process. It is important to note that data from which only the names are removed is not de-identified, an individual is potentially identifiable due to the presence of other factors (identifiers) such as an address, date of birth, postal code, etc.

In addition to ethical considerations, legal requirements, such as those required under the Data Protection Acts 1988 to 2003 and all requirements under GDPR, apply to the collection and storage of personal information. Advice available from both UCD GDPR Office http://www.ucd.ie/gdpr/ and the University Records Manager: http://www.ucd.ie/dataprotection/index.html