PD-Net Ethics Primer

# Introduction

This ethics primer is intended for PD-Net project members and provides an introduction to ethical issues in research involving studies and experiments with humans. It also outlines the ethical assessment process adopted in PD-Net.

Ethical guidelines on human subject experiments provide guidance on how to properly treat human subjects and their data. While computer science typically does not concern itself with experiments in the same way that, say, medicine or psychology does (i.e., directly experimenting *upon* individuals), many of our studies will ultimately collect and store information that may or may not be associated with individuals. This information may inconvenience or even threaten the physical and psychological well-being of test subjects, should it be used for unforeseen purposes or be shared with unintended recipients. For example, if usage measurements of how an employee uses work-related software would leak, his or her employer might learn of substandard performance, hidden attitudes, or detect obvious errors in conduct. By following the ethical principles set forth in this handbook, work in PD-Net should minimize potential threats to human subjects stemming from project-related user studies.

Use the table of contents below to locate relevant information in this document. Of particular interest is the PD-Net Ethical Assessment Process (page 4) and the fundamental Ethical Principles (page 4) that research within PD-Net follows.

**Table of Contents**

[Introduction 1](#_Toc277607235)

[Ethics Background 2](#_Toc277607236)

[Ethical Assessment Process 4](#_Toc277607237)

[Ethical Principles 4](#_Toc277607238)

[Overview 5](#_Toc277607239)

[Definitions 5](#_Toc277607240)

[Principles Explained 6](#_Toc277607241)

[Bibliography 9](#_Toc277607242)

# Ethics Background

There is a vast amount of literature on ethics, ranging back to Plato and Aristotle. However, Mackay [2] points out that modern professional ethics codes in the field of computer science are mostly influenced by two relatively modern perspectives: Mill’s *utilitarianism*, and Kant’s *deontologism*.

Deontological Ethics (deon is Greek for “duty”, logos means “science”) infers moral obligations from the characteristics of a certain action, without regard for its consequences. Thus, an action that is morally good might still have serious negative consequences. One of the most prominent proponents of deontological ethics was Immanuel Kant, who formulated a “Golden Rule,” his categorical imperative, for determining the morality of an action:

Act only on that maxim whereby thou canst at the same time will that it should become a universal law.

Note that Kant’s Golden Rule is not just a reformulation of the Biblical Golden Rule “All things whatsoever you would have men do unto you, do you ever so to them,”[[1]](#footnote-1) as it explicitly requires moral principles to be universally applicable, to become a universal law of nature. It is thus a categorical imperative, not just a hypothetical imperative, which only applies conditionally (e.g., only if you want people to do A to you, do A to them).

Teleological Ethics on the other hand, derives morality not from the intentions, but from the consequences of actions, e.g., whether it leads to “desirable” effects (telos is Greek for “goal” or “end”). In the context of a research study, this could for example be taken to allow for the deception of study subjects if it would lead to more relevant results, while not negatively affecting the subjects. The exact nature of these effects, i.e., what exactly constitutes a desirable effect, is of course no less debated than the moral truths of the deontologists.

The most prominent teleological ethical theory is that of *utilitarianism*. Its main proponents were the late 18th- and 19th-century English philosophers Jeremy Bentham and John Stuart Mill. John S. Mill was an ardent proponent of the freedom of individuals from government interference. In his 1859 essay *On Liberty*, Mill proposed as the proper balance between individual liberty and governmental authority the “harm principle:”

[T]he only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others [241].

Professional Codes from, e.g., the *National Society of Professional Engineers* or the *Association for Computing Machinery* (ACM)[[2]](#footnote-2) try to give practical guidance to their members through publishing a Code of Ethics for their respective fields (see Table 1 on the next page). They are typically a mixture of deontological (“be honest and trustworthy”) and teleological (“contribute to society and human well-being”) approaches. Table 1 below lists the “moral imperatives” from the ACM Code of ethics.

**Table 1**: ACM Code of Ethics – Moral Imperatives (excerpt from [www.acm.org/constitution/code.html](http://www.acm.org/constitution/code.html)). Professional associations such as the ACM use Codes of Ethics to provide practical ethical guidance to their members. They are typically a mixture of deontological and teleological approaches.

1. **Contribute to society and human well-being**. When designing or implementing systems, computing professionals must attempt to ensure that the products of their efforts will be used in socially responsible ways, will meet social needs, and will avoid harmful effects to health and welfare
2. **Avoid harm to others**. To minimize the possibility of indirectly harming others, computing professionals must minimize malfunctions by following generally accepted standards for system design and testing. Furthermore, it is often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others.
3. **Be honest and trustworthy**. Honesty is an essential component of trust. Without trust an organization cannot function effectively. The honest computing professional will not make deliberately false or deceptive claims about a system or system design, but will instead provide full disclosure of all pertinent system limitations and problems.
4. **Be fair and take action not to discriminate**. Discrimination on the basis of race, sex, religion, age, disability, national origin, or other such factors is an explicit violation of ACM policy and will not be tolerated.
5. **Honor property rights including copyrights and patent**. Violation of copyrights, patents, trade secrets and the terms of license agreements is prohibited by law in most circumstances. Even when software is not so protected, such violations are contrary to professional behavior.
6. **Give proper credit for intellectual property**. Computing professionals are obligated to protect the integrity of intellectual property. Specifically, one must not take credit for other’s ideas or work, even in cases where the work has not been explicitly protected by copyright, patent, etc.
7. **Respect the privacy of others**. This imperative implies that only the necessary amount of personal information be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s).
8. **Honor confidentiality**. The principle of honesty extends to issues of confidentiality of information whenever one has made an explicit promise to honor confidentiality or, implicitly, when private information not directly related to the performance of one’s duties becomes available.

While professional code offer a more practical approach to ethical theory, they still fail to prescribe practical steps to be taken when planning and conducting a user study or performing an observation in the field. As a consequence, this primer prescribes a concrete set of principles to follow when designing, conducting, and analyzing field trials, user studies, and other experiments involving human study subjects. However, the above principles (see Table 1) should be taken as overarching principles that should guide all actions of PD-Net researchers during all stages of the project.

# Ethical Assessment Process

The list below outlines the steps that all user studies, observations, field trials, and interviews planned and performed in the context of PD-Net should follow.

1. Fill out *PD-Net Ethical Worksheet* **prior** to planned begin of study
	1. Prepare Consent Form if needed (see PD-Net Guide to Informed Consent)
2. If needed, seek local approval from local *Institutional Review Board* (IRB) and regulatory bodies
	1. If IRB assessment required, prepare necessary documents and submit
	2. If regulatory approval required, prepare necessary documents and submit
	3. Incorporate any feedback, resubmit if necessary
3. Identify type of research and consult set of appropriate *PD-Net Study Process Template* (SPT) for process
	1. If no PD-Net SPT matches, create new PD-Net SPT for this class of research and submit to PD-Net *Ethical Review Board* (ERB) **prior** to planned begin of study
		1. Incorporate any feedback from ERB, resubmit to ERB if necessary
		2. Complete PD-Net Worksheet with results from ERB, IRB, regulatory assessments
4. If new IRB approval and/or ERB assessment, submit results to PD-Net Coordinator prior to planned begin of study

Proceed with the planned study only if all relevant PD-Net SPTs have been approved by the ERB and all local IRB issues (if applicable) have been addressed.

# Ethical Principles

Studies and observations in PD-Net follow the 10 basic principles outlined below.[[3]](#footnote-3) Individual types of studies and how these principles apply are described in a separate set of guides, the so-called “PD-Net Study Process Templates” (SPT). There is, e.g., the *PD-Net Procedures Public Trials* or the *PD-Net Guide to Volunteer Studies*. There are also guides to general principles such as the *PD-Net Guide to Obtaining Informed Consent* and the *PD-Net Guide to Secure Data Storage*.

See also the section describing the Ethical Assessment Process on page 4 for details on how these guidelines are used in practice, in particular the role of the PD-Net Ethical Review Board.

## Overview

1. Maximize Possible Benefits and Minimize Possible Harms
2. Obtaining Voluntary Informed Consent
3. Ensuring Right to Withdraw
4. Disclosing Detriment Arising from Participation in Research
5. Providing Data Protection and Privacy
6. Limiting Disclosure
7. Following Minimal Intrusion Principle
8. Offering Adequate Incentives
9. Special Provisions for Experiments Involving Children and other Vulnerable People
10. Avoiding Deception

## Definitions

* The **participants** in research may be the active or passive subjects of such processes as observation, inquiry, experiment or test. They may be collaborators or colleagues in the research process or they may simply be part of the context e.g. where passers-by are part of the context but not the subjects of an on-campus study on (adapted from: [1])
* **Personally identifiable information** (PII) is data that can – with reasonable effort – be *linked* to an individual. Linking requires that a person can be distinguished – with more or less certainty – from all other persons. Examples of PII are, e.g., the first and last name; a home or other physical address including street name and name of city or town; an email address; and a telephone number. Also a seemingly random identifier, such as an IP address or a **Bluetooth MAC** address, can become PII, if these can in turn be linked to any other PII such as a physical address. The information necessary to perform the linking may be in another (local) database, in the public domain (e.g., white pages), or can be obtained with reasonable effort from another (remote) database. Note that much depends on the size of the potential user population: if an experiments involves only members of a particular department, then knowing even a relatively innocuous data point such as “height” may already constitute PII.
* **Anonymisation, pseudonymisation and identifiability** (from [4]): ‘Anonymous’ often means data which does not identify an individual; ‘anonymised’ means data which has been rendered anonymous; ‘pseudonymised’ and ‘coded’ means data where obvious identifiers (e.g. names and addresses) have been replaced with indirect identifiers (e.g. numbers) in the main data set and the indirect identifiers are then held with the obvious identifiers in a separate data set (known as the ‘key’). The key term underlying all of the above definitions in the context of European data protection law is the ‘identifiability’ of an individual from the data. For European data protection law to bind research on personal and sensitive personal data one must ask: is the individual identified either immediately from the data or when that data are combined with other data in the hands of another person. This combination extends only to *reasonably foreseeable* linkings of data. Therefore, data which is gathered anonymously without any identifiers will be outside the scope of European data protection law; data which is pseudonymised or coded will be within the scope of the law as it is possible to reintroduce the two separate data sets and identify individuals; data which was gathered as identifiable data and then anonymised is subject to the data protection legislation when it contains identifiable data (most importantly at the point of gathering the data, requiring the disclosure by the researcher to the research participant of information including the purpose of the processing and contact details).
* **Sensitive information** (from [5]). Sensitive data include data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" (Article 10 of Regulation 45/2001; Article 8 of Directive 95/46/EC). The processing of such information is in principle prohibited, except with the explicit consent of the data subject. Processing and storing sensitive information requires a significantly increased level of security (adequacy principle – see the *PD-Net Guide to Secure Storage*).

## Principles Explained

### Do No Harm

One of the most fundamental principles of ethical research is the harm principle. It stems from the 1979 Belmont report [7], which identifies basic ethical principles that should underlie all types of behavioral research involving human subjects. The report lists three basic principles: Autonomy, Beneficence, and Justice. The last principle (justice) simply states that both the risks and the benefits of research should be distributed equally. This may become relevant, e.g., when selecting participants. The Beneficence principle then obligates the researcher to secure the well-being of all selected participants, i.e., to “maximize possible benefits and minimize possible harms.” In practice, each study in PD-Net must explicitly list possible risks to participants and explain how their adverse affects are mitigated (e.g., involuntary disclosure of personal data). This information must also be communicated to potential participants *prior to enrolment*, which supports the first of the three principles, Autonomy, and which is explained in the next item below.

### Informed Consent

The first of the three Belmont principles, Autonomy, stipulates that each participant should be given the respect, time, and opportunity necessary to make his or her own decisions, in order to “make sure they undertake activities freely and with awareness of possible adverse consequence.” This principle is implemented through a so-called *Informed Consent* process. Consent to participate in research is a process, rather than an event [3]. Researchers should plan for and outline how consent is initially obtained and how it is reviewed throughout the study. Also, in order to give meaningful consent, participants must understand the goals of the research, the study/experiment to be performed, the data that is collected, and the uses of this data. While written consent is preferred, oral consent might be more appropriate in some situations, e.g., walk-up interviews on public places. Note that the principle of informed consent includes the principle of disclosing detriment and ensuring the right to withdraw (see below). A detailed description of the informed consent process in PD-Net can be found in the *PD-Net Guide for Obtaining Informed Consent.*

### Right to Withdrawal

As part of the informed consent procedure outlines above, potential participants must be informed of the right to refuse to participate in the study, and that they can withdraw their consent to participate at any time without reprisal [8]. This should include the right to withdraw retrospectively, i.e., in the light of experience of the investigation, or as a result of debriefing. Any such request should result in the destruction of the participants own data. Note that the unconditional right to withdrawal has been questioned repeatedly by researchers [9][10], as it might not only prevent researchers from encouraging study subjects to continue participation, but also lead to a prior dismissal of potential drop-outs from the pool of study participants. As described in the informed consent principle above, researchers in PD-Net should seek an ongoing dialog with participants throughout the study, in order to ensure that while proper information is given regarding withdrawal, participants are adequately encouraged to continue.

### Disclosing Detriment

Disclosing possible detriments arising from participation is an integral part of obtaining informed consent from potential study participants. As part of the *PD-Net Ethical Worksheet*, researchers in PD-Net will have to explicitly list the risks to study subjects that could stem from participation. This information must explicitly be disclosed to participants in the informed consent documents.

### Privacy

Data collection, storage, and use of personally identifiable information (PII) in PD-Net in general must follow the EU legal framework (i.e., the 1995/46/EC Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data), as well as individual national legislation on data protection. Legal requirements on processing PII typically comprise the following aspects, roughly modeled after the OECD Guidelines of 1980 [11]:

1. Notice—data subjects should be given notice when their data is being collected;
2. Purpose—data should only be used for the purpose stated and not for any other purposes;
3. Consent—data should not be disclosed without the data subject’s consent;
4. Security—collected data should be kept secure from any potential abuses;
5. Disclosure—data subjects should be informed as to who is collecting their data;
6. Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; and
7. Accountability—data subjects should have a method available to them to hold data collectors accountable for following the above principles

The principles of notice, consent, and disclosure are covered by PD-Net’s informed consent process (see the *PD-Net Guide for Obtaining Informed Consent*). The purpose principle is addressed through the rigorous use of *Ethical Worksheets* explicitly describing the individual study goals. Security is ensured by following the PD*-Net Guide for Secure Storage*, and by explicitly stating the data storage and processing circumstances for each individual study in the *Ethical Worksheet*. Access and accountability are given by including access and inspection methods into the information sheet administered as part of the informed consent (e.g., the contact information of the Principle Investigator responsible for the study, as well as the contact details of the PD-Net Ethical Review Board and – if applicable – any local institutional review board).

In addition, European data privacy laws require the proportionality/data minimization principle – see the “Minimal Intrusion Principle” listed below.

### Limiting Disclosure

Personally identifiable data collected as part of a study in PD-Net will only be made available to researchers directly involved with the research, on a “need to know” basis. The *PD-Net Ethical Worksheet* asks researchers to explicitly list all members of the consortium who will participate in the administration of a particular study, as well as any outside researchers.

### Minimal Intrusion Principle

The principle of “minimal intrusion” or “data minimization” means that a one should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. Data should also be retained only for as long as is necessary to fulfill that purpose. This principle derives from Article 6.1(b) and (c) of Directive 95/46/EC , which provide that personal data must be "collected for specified, explicit and legitimate purposes" and must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed". This also often referred to as the proportionality principle, i.e., “whether the means employed by the measure to be evaluated are suitable and reasonably likely to achieve its objectives” [12]. In the context of PD-Net research, this means that researchers should only collect information that provides the data required to address current research questions. The *PD-Net Ethical Worksheet* asks researchers to explicitly state what data should be collected in a study (question 3.6), and requires a justification on the suitability of this data (and the study methods employed) for the stated research purpose (question 3.4).

### Adequate Incentives

The use of incentives to recruit and retain research subjects is typically rather innocuous. However, when study subjects are in a dependency relationship with the researcher (e.g., students in a course), or when the participant’s aversion to the study may be strong (e.g., high risk, degrading research, aversion on principle) [13]. In the context of PD-Net, incentives should only comprise adequate compensation for the participants’ time and efforts, e.g., for coming to weekly meetings. If necessary, small incentives in the form of vouchers for online stores such as Amazon.com or iTunes may be given, or all participants enter into a drawing of a small set of prizes.

### Avoiding Deception

The act of deceiving study participants is often used in psychological experimentation, in order to ensure that study subjects do not inadvertently change their “natural” behavior in order to please the experimenter and/or to make themselves appear in a better light. Infamous examples of deceptive experiments are the Stanley Milgram experiment of 1974 [14] or Zimbardo’s Stanford Prison experiment of 1971 [15]. Today, as a general rule, deception is not acceptable when doing research with humans. Using deception jeopardizes the integrity of the informed consent process and can potentially harm participants. Should the use of deception become necessary in any field study within the scope of PD-Net, explicit approval by an institutional review board (if available) should be sought. If possible, the PD-Net ethical review board should also be asked for comments (e.g., using the PD*-Net Ethical Worksheet* for describing the experiment).

The use of deception requires an in-depth justification of why the deception is necessary for the study, and the steps taken to safeguard study participants.

### Vulnerable Participants

Vulnerable participants are those unable to give their unambiguous informed consent, such as children, people with cognitive disorders, or those with cultural or intellectual difficulties in speech and understanding. Experiments seeking the participation of vulnerable participants must be justified and get prior approval of an appropriate institutional review board, and, if possible, obtain feedback from the PD-Net ethical review board. Informed consent must be obtained from parents or other appropriate legal guardians.

# Bibliography

1. British Educational Research Association (bera): **Revised Ethical Guidelines for Educational Research**, 2004. Available from <http://www.bera.ac.uk/files/guidelines/ethica1.pdf>
2. Mackay, Wendy E.: **Ethics, Lies and Videotape...** In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Denver, Colorado, United States, May 07 - 11, 1995. ACM Press/Addison-Wesley Publishing Co., New York, NY, pp.138-145. DOI: [10.1145/223904.223922](http://doi.acm.org/10.1145/223904.223922)
3. UofT Research Ethics Board (REB): **Guide for Informed Consent**. University of Toronto, Canada, April 2010.
4. Caroline Gans-Combe (ed.): **Data Protection and Privacy Ethical Guidelines** (Version 5). European Commission, September 18, 2009
5. The European Data Protection Supervisor (EDPS): Data Protection Glossary. The EDPS Website. See <http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Glossary>
6. Eléonore Pauwels: **Ethics for Researchers. Facilitating Research Excellence in FP7**. See ftp://ftp.cordis.europa.eu/pub/fp7/docs/ethics-for-researchers.pdf
7. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research: **The Belmont Report - Ethical Principles and Guidelines for the Protection of Human Subjects of Research.** U.S. Department of Health, Education, and Welfare, 1979. See <http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.htm>
8. World Medical Association: **WMA Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects**. 18th WMA General Assembly, Helsinki, Finland, 1964. See <http://www.wma.net/en/30publications/10policies/b3/index.html>
9. Sarah J. L. Edwards: **Research participation and the right to withdraw**. Bioethics. 2005 April; 19(2):112-30. DOI: [10.1111/j.1467-8519.2005.00429.x](http://onlinelibrary.wiley.com/doi/10.1111/j.1467-8519.2005.00429.x/full)
10. Stefan Eriksson and Gert Helgesson: **Potential harms, anonymization, and the right to withdraw consent to biobank research.** European Journal of Human Genetics (2005) 13, 1071–1076. doi:10.1038/sj.ejhg.5201458; published online 29 June 2005. See <http://www.nature.com/ejhg/journal/v13/n9/abs/5201458a.html>
11. Organization for Economic Co-Operation and Development: **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.** See [http://www.oecd.org/document/18/0,2340,en\_2649\_34255\_1815186\_1\_1\_1\_1,00.html](http://www.oecd.org/document/18/0%2C2340%2Cen_2649_34255_1815186_1_1_1_1%2C00.html)
12. Christopher Kuner: **Proportionality in European Data Protection Law And Its Importance for Data Processing by Companies**. Privacy & Security Law Report, Vol. 07, No. 44, 11/10/2008, pp. 1615ff.
13. Ruth W. Grant and Jeremy Sugarman: **Ethics in Human Subjects Research: Do Incentives Matter?** Journal of Medicine and Philosophy, 29(6): 717–738, 2004. See <http://www.waisman.wisc.edu/EVENTS/ethics/sprin06-sem2-incentives-compensation.pdf>
14. Stanley Milgram: **Obedience to Authority**. New York: Harper & Row, 1974
15. Philip G. Zimbardo: **The power and pathology of imprisonment**. Congressional Record. (Serial No. 15, 1971-10-25). Hearings before Subcommittee No. 3, of the Committee on the Judiciary, House of Representatives, Ninety-Second Congress. Washington, DC: U.S. Government Printing Office.
1. See (Matthew 7:12) [↑](#footnote-ref-1)
2. See [www.nspe.org](http://www.nspe.org) and [www.acm.org](http://www.acm.org), respectively. [↑](#footnote-ref-2)
3. Principles taken from [1], [↑](#footnote-ref-3)