Ethical issues, data protection and privacy in the 7th Framework Program

Reihoo
Director - Program Manager
Caroline Gans Combe
Are data protection and privacy ethical issues?

Let’s try to define these different concepts

- **Ethics** is the branch of philosophy that defines what is good for the *individual* and for *society* and establishes the nature of obligations, or duties, that people owe themselves and one another. In other words, ethics define how individuals, professionals, and corporations choose to *interact* with one another.

- **Privacy** is the interest that *individuals* have in sustaining a 'personal space', free from interference by other people and *organizations*.

- **Data protection** consists of a technical framework of security measures designed to guarantee that data are handled in such a manner as to ensure that they are safe from unforeseen, unintended, unwanted or malevolent use.
Going deeper into privacy

- **A four dimensions concept:**
  - **privacy of the person** takes into account issues about the right of each individual to have the integrity of his/her body protected.

  - Persons should not be coerced into providing any kind of fluids or biological samples, being given blood transfusion without consent, being subjected to any kind of chirurgical intervention without consent (invasive techniques within research),

  - **privacy of personal behavior** relates to all aspects of behavior, but especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices, both in private and in public places,

  - **privacy of personal communications**. Individuals should be able to communicate among themselves, using various media, without monitoring of their communications by other persons or organizations.

  - **privacy of personal data**. Data about individuals should not be automatically made available to other individuals and organizations even when data is possessed by another party. Each person must be able to exercise a substantial degree of control over that data and its use.
When ethics meet data protection and privacy
### Targets of the ethical issues Table (EIT) on data protection and privacy issues

- **Ethics** define the way individuals and/or groups of individuals choose to interact between one another
  - Social best practices...
- **Privacy** defines the four universes where this interaction should be fine-tuned:
  - privacy of the person, privacy of personal behavior, privacy of personal communications, privacy of personal data...
- **Data protection** consists in the technical methods to do so....

*Privacy Protection* is a process of finding appropriate balances between privacy and multiple competing interests.

Therefore, the main objective of the EIT is to **explain how, within the planned research, this appropriate balance is put into practice and maintained**.
Being pragmatic: let’s fill the EIT on a data protection and privacy point of view

- **Rule 1** – when human subjects are at stake, even under the form of samples, there are data protection and privacy issues.

- **Rule 2** – it is not enough to tick the proper line in the form, this shows identification but not assessment nor processes.

- **Rule 3** – each applicant needs to be prepared to explain processes and methodologies used for data and samples processing within the ethical section.
Rule 4 – There is not one way to take into account data protection and privacy issues, but several according to the legal environment of each country: to make things short, if the said country has a legal system based on common or civil law.

- In civil law, the legal framework delivers a process to be followed on compulsory basis, and each citizen is supposed to comply.
- In common law, no formal fixed references are supposed to exist, only guidelines for data protection and privacy documents will be delivered.
- In some case, declaration and administrative process might not even exist at all.
- Applicants need to determine is if a proper authority exists, what is its role and what – according to the legal environment in which such authority or competent bodies act – are the compulsory legal actions to be undertook on data protection and privacy issues.
Depending of the legal environment, either to declare to a proper authority (if existent) the nature of the content that will be stored under electronic means or not, and what will be done of such data or to establish a document demonstrating that they are compliant with the local guidelines;

To submit - or to be prepared to submit - to the proper authority/competent body a risk management and disaster recovery process in order to prevent malevolent use or unwanted access.

Being pragmatic: what are the legal requirements when using data (electronic or not)?
Informed Consent

<table>
<thead>
<tr>
<th>Informed Consent</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Does the proposal involve children?</td>
</tr>
<tr>
<td>• Does the proposal involve patients or persons not able to give consent?</td>
</tr>
<tr>
<td>• Does the proposal involve adult healthy volunteers?</td>
</tr>
<tr>
<td>• Does the proposal involve Human Genetic Material?</td>
</tr>
<tr>
<td>• Does the proposal involve Human biological samples?</td>
</tr>
<tr>
<td>• Does the proposal involve Human data collection?</td>
</tr>
</tbody>
</table>

**Informed consent is not just about patients**

- Informed consent can be define as an agreement to do something or to allow something to happen, made with complete knowledge of all relevant facts, such as the risks involved or any available alternatives.

- On a data protection and privacy issues’ point of view, all subjects present in a project - from patients to co-workers - need to be informed of what will be done with the data gathered about them, whatever the data is, and whatever the data is for.
• To provide an information document to each research subject/or participant stating:
  ➔ Which data is going to be collected,
  ➔ What for,
  ➔ How the data will be used, exchanged,
  ➔ How the data will be archived,
  ➔ What will be the duration of data conservation,
  ➔ How is organized the right to retreat,
  ➔ How is the data treated in case of retreat,
  ➔ When, if convenient, the data will be destroyed.

• To gather by any mean the authorization of the research subject to the above usage. The used means can be (this list is of course indicative and not limitative):
  ➔ Online opt in
  ➔ Electronic signature of a document
  ➔ Formal form signature
Privacy

<table>
<thead>
<tr>
<th>Privacy</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the proposal involve processing of genetic information or personal data (e.g. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)</td>
<td></td>
</tr>
<tr>
<td>Does the proposal involve tracking the location or observation of people?</td>
<td></td>
</tr>
</tbody>
</table>

- The main question - Is the gathered data really needed?
  - Not all data is needed in order to deliver results within a research project. For example, if a survey needs to be done, the full identity of the participants is not really needed. What is needed is their general socio-economic profile as well as input.
  - ID information must be reduced to a minimum in order to insure a correct interpretation of results, a correct treatment of incidental findings and a strict protection of the subject.

- Projects’ proposers must be aware that privacy not only concerns the project’s subjects, but also on a whole, the perimeter of the project.
  - The way data is treated impacts not only the subjects of a research but also the different workers involved within the actual research such as researchers, lab workers and so on.

- There is a link between privacy and informed consent in the EIT...if you tick one, you might need to tick the other.
• Applicants need to anticipate if, taken from another angle than her/his own, the data developed within the research project is in a way sensitive. This is even more important as data with a potential dual use are subjected to specific treatment and controls.

→ Does the data within the project can have another usage?

→ If this is the case, are the proper measures to protect and control data flow taken?

→ If this is the case, are the proper authorizations for data circulation obtained or in the process of being obtained?
Research involving Developing countries, data protection and privacy

- It is not because a research is implemented outside Europe that the European standards are not applied... Therefore, applicants are supposed to implement their project the European legal standards and processes.

- Applicants need to be particularly cautious concerning the “use of local resources” section in the Ethical issues form, as test populations are local resources, as well as populations used within surveys.

- If this section is ticked, applicants must check if the participation of the developing countries implies data protection and privacy issues, and complete adequately the form.

- This is particularly important when using pre-existing data as it is not certain that the proper measures were taken in order to take care, for example, of incidental findings or confidential data protection. This aspect is vital when diseases are at stake as knowledge of an infection can lead – in certain cultures - to ostracism toward the infected person.


07/05/2009
Technical aspects beyond privacy: data protection

ATTENTION VIRGINIA

I have your shit! In *my* possession, right now, are 8,257,378 patient records and a total of 35,548,087 prescriptions. Also, I made an encrypted backup and deleted the original. Unfortunately for Virginia, their backups seem to have gone missing, too. Uh oh :(

For $10 million, I will gladly send along the password. You have 7 days to decide. If by the end of 7 days, you decide not to pony up, I'll go ahead and put this baby out on the market and accept the highest bid. Now I don't know what all this shit is worth or who would pay for it, but I'm bettin' someone will. Hell, if I can't move the prescription data at the very least I can find a buyer for the personal data (name, age, address, social security #, driver's license #).

payin out, but I suggest that policy be turned right the

Please send me a line at hackingforprofit@yahoo.com and we can
Technical aspects beyond privacy: data protection

- **Data storage:** Data storage is the process of providing storage of and access to data whatever the form under which the data is. Data storage must be secured, that is:
  - Not accessible to unwanted third party,
  - Protected against disaster and risk.

- Different topics that should be considered:
  - Where is the data stored?
  - On which hardware type is the data stored: paper, disk, removable device?
  - Who has access to the data? For how long will the data be stored, accessed?
  - Can the data be accessed by any third party? Can the data be copied by any third party?
  - If stored on a machine, does the storage machine/server is equipped with: Wifi, Bluetooth, Usb drive

Answers to these questions will help the applicants to assess the data protection and privacy risks within the project and therefore provide a state of the art risk management policy.
**Technical aspects beyond privacy: data protection**

- **Data structure & circulation trends**
  - Data is a living material.
  - Data is supposed to circulate within different users, or to be completed and enriched by different users.
  - This need to circulate also opens the door to data theft and different malevolent usage.
  - This can be fought by rendering data access difficult, or data unusable by unwanted third parties.

- **In order to do so, two questions need to be asked.**
  - How is the data structured?
  - Will the data circulate within the project, will the data be delivered to any third party, is this data circulation strictly needed?

In other words, is the information flow properly split should such flow be used for several purposes.
• A data protection and privacy glossary in order to identify the main ethical aspects of data protection and privacy within a research;

• A data protection and privacy guidelines,

• A data protection and privacy checklist in order to assist each applicant while filling the ethical table on data protection and privacy issues
Thank you for your attention