Guidelines on the protection of children's personal data

May 2011

INTRODUCTION

The history of clinical research on children reveals an especially vulnerable population needing special protection against violation of individual rights and exposure to undue risk. The development of guidelines and policies to protect children as research subjects is necessary. The need of new guidelines may represent a return of the pendulum to a more moderate position, after an era of restrictive regulations in reaction to past abuses of children as research subjects. Children represent more than 20% of the European population, with about 100 million people aged less than 19 years. The lack of specific drugs and labelling recommendation for the paediatric population is a long-standing worldwide problem and evidence-based prescribing for children is compromised by lack of satisfactory efficacy and safety data on many drugs: 50% to 75% of medicines used in children have not been studied adequately in the paediatric population. [**1**] As a result, different initiatives renewed the focus on the need for rigorous study of childhood development and disease within an appropriate ethical framework. [**2**]

Compared to the US, the EU experience in paediatric research is less extensive. In the field of child and adolescent psychopharmacology, the majority of publications and studies are coming from the US. Reviewing 27 placebo-controlled trials assessing the use of antidepressant medications among more than 4400 children and adolescents published between January 1998 and July 2006 in Medline, Apter et al. reported that 23 out of 27 were conducted solely in the US and only 3 were done partly in European countries. The public perception of paediatric research in Europe and the awareness of Ethics Committees is still controversial. [**3**].
Generally, the barriers to undertake proper research on children's drugs development include:

- the cost of studies compared with the size of the potential market which implies that conducting research on medicines for children is often financially unrewarding for the pharmaceutical companies; difficulties in trial design (i.e., small numbers of eligible patients and lack of appropriate age-matched controls);
- time taken to complete studies in children as compared in adults;
- long approval processes;
- unique and complex ethical issues surrounding research on children;
- assessment of risk-benefit in those who cannot provide consent for themselves.

The new European legislation, entered into force in January 2007 [**4**]. help the development of networks of EU centers for clinical research stimulating identification and training of investigators in child and adolescent psychiatry.

One of the most important issue is the use of the child's personal data.

As reported in the Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms "Everyone has the right to respect for his private and family life, his home and his correspondence", so also a child, who is a human being in the complete sense of the word, has the right to the protection of his own personal data (article 29 WP147, 2008).
The use of personal data is, crucial to carry out a clinical research, but since the consent to the use of their personal data is given by their parents or legal guardian, children need a "special" protection . Because of their relative immaturity, but irrespective of whether they are competent to make their own treatment decisions; therefore they should not be permitted to make major decisions which will seriously harm them (Article 3: 2, UN Convention of the Rights of the Child).
In fact, children, with the exception of the emancipated minor*, are able to give only their assent.

When children and young people suffer from mental or physical disorders, they become more vulnerable and the issue of protection becomes even more important [**3**]..

KEY POINTS

"Paediatric population" refers to the part of the population aged between birth and 18 years.

Paediatric population is vulnerable and need "special" protection

The protection of children's personal data has to be guaranteed

Parents/legal guardians are responsible of giving the consent for the treatment of their children's personal data

PURPOSE AND SCOPE

"*It is the duty of physicians who participate in medical research to protect the life, health, dignity, integrity, right to self-determination, privacy, and confidentiality of personal information of research subjects*" (World Medical Association Declaration of Helsinky, Ethical Principles for Medical Research Involving Human Subjects, Seoul October 2008) .

The European Commission identified children's rights as one of the **main priorities:** "A particular priority must be effective protection of the rights of children, both against economic exploitation and all forms of abuse"(Communication on Strategic Objectives 2005-2009).
Although "All forms of abuse" include also the **unfair use** of their personal data, the relevant European Directive on data protection, 95/46/EC and 2002/58/EC, do not explicitly mentioned the privacy rights of minor. The Working document 1/2008 on the protection of children's personal data (General guideline and the special case of schools) of the Article 29 Data Protection Working Party, on the other hand, offers an important guidance for the protection of children's data, especially in the field of school. This Working document has the aim of improving the practical aspects of ethical issue of paediatric research by strengthening the fundamental right of children to the protection of their own personal data (article 29 Data Protection Party, 2008) when involved in clinical research.

The present guidelines are prepared according to the following European data protection directives and guideline:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Working Document 1/2008 on the protection of children's personal data (article 29 Data Protection Party, 2008)

The present guidelines are prepared also considering the national laws of the countries involved in the STOP project, trying, as possible, to harmonise them for the purpose of the project:

- Data Protection Act 1998, United Kingdom
- Dutch Data Protection Act 2001 , Netherlands

- Federal Data Protection Act (BDSG) In the version promulgated on 14 January 2003 (Federal Law Gazette I, p. 66), last amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I p. 2814)],p. 2814), Germany
- Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004) [Act n° 78-17 of January 1978 on data processing, data files and individual liberties (amended by the act of 6 august 2004 relating to the protection of individuals with regard to the processing of personal data and by the act of 12 may 2009 relating to the simplification and clarification of law and lightening of prdocedures], France
- Ley oroganica 15/1999, de 13 de diceimbre, de proteccion de datos de caracter personal (Cambio denominación por artículo 79 Ley 62/2003, de 30 de noviembre: Las referencias a la Agencia de Protección de Datos deberán entenderse realizadas a la Agencia Española de Protección de Datos), [Oganic Law 15/1999 of 13 December on the Protection of Personal Data], Spain
- Decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali, [Decree Legislative 30 June 2003, n.196 Code for the Protection of Personal Data], Italy)

These guidelines are mainly addressed to the protection of personal's data of children/adolescents involved in clinical research, by providing investigators the knowledge and the means that are fundamental to guarantee the protection of patients' personal data and the respect of their privacy.

This document provides the general tools to protect personal data of patients involved in the STOP project, and specific tools referred to the prospective cohort studies on Risperidone (WP 7) Fluoxetine (WP 8), and on Montelukast (WP 9).

A dedicate guideline will be provided for the collection of biological sample.

KEY POINTS

Purpose: providing specific knowledge and instruments for the correct use of minors' personal data according to European directives

GUIDANCE based on Directive 95/46/EC

1. Data quality

For what purpose the data can be data collected?
For specified, explicit and legitimate purposes and NOT further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or SCIENTIFIC purposes shall not be considered as incompatible.

What features should they have?
Adequacy, relevance, and not to be excessive in relation to the purpose for which they are collected and/or further processed; accuracy, and when necessary, kept up to date

How long they have to be retained?
No LONGER than it is necessary for the purposes for which the data were collected or for which they are further processed, (or better the data must be kept in form which permits identification of data subjects for NO longer than is necessary).

KEY POINTS

'Personal data' are data related to any personal information which can be used to identify the person, directly or indirectly, such as name, telephone number, email address, place and date of birth, etc.

Children's personal data can be collected and processed for specified, explicit and legitimate scientific purposes

Personal data must be adequate and relevant for the purpose to gain (according to the protocol)

Personal data have to be kept up to date

Personal data must be kept for NO longer than it is necessary or

Personal data must be made anonymous (it is used a code and it is impossible to link this code with the person)

2. Legitimacy of processing data

Who does legitimate the process of the data?

The data may be processed only if the subject has given his consent.

According to the Declaration of Helsinky some research populations are particularly vulnerable and need special protection. These include those who cannot give or refuse consent for themselves, such

as children and adolescents. In fact as a rule, a paediatric subject is legally unable to provide informed consent.

Informed consent to participate in research studies is defined by the Good Clinical Practice (ICH Topic E 6 (R1)) as a process by which a subject voluntarily confirms his or her willingness to participate in a particular trial, after having been informed of all aspects of the trial that are relevant to the subject's decision to participate. Informed consent is documented by means of a written, signed and dated informed consent form.

Children/adolescents are dependent on their parent(s)/legal guardian to assume responsibility for the use of their data. Fully informed consent should therefore be obtained from the legal guardian in accordance with national /regional laws or regulations. All participants should be informed to the fullest extent possible about the use of their data in language and terms they are able to understand.
Where appropriate, minor participants should assent to the use of their data. It is important to provide to parents/legal guardian all the information referring the collection and the processing of their son's data. Minors will be provided all the information referring the collection and processing of their data according to their level of maturity, in order to give their assent. Participants of appropriate intellectual maturity should personally sign and date either a separately designed, written assent form or the written informed consent.(ICH Topic E 11).
Strong and definitive objections from the child should be respected.

If an adolescent aged 16 to 18 is no longer a minor as defined in national law, or is an "emancipated minor", then written informed consent is required from these individuals as for any adult capable of giving consent. Under these conditions, informed consent is no longer required from the parents/legal representative, although an adolescent is still vulnerable and may require additional discussions and explanations and every effort should be made to understand and respect differences of opinion between the child and his/her parents or legal representative.

KEY POINTS

Minor is legally unable to provide informed consent

Informed consent must be written, signed and dated by both parents/ legal guardian

Minor should assent for the use of their data from the intellectual age of 7 years

Assent means the acceptance of an approach or action that is offered without a full and comprehensive exploration of the alternatives and it is given by a person who may not be fully capable of consent but may be clear about his or her wishes.

Strong and definitive objections from the child should be respected

3. Security of data (included electronic data)

How the data should be retained safely?
The controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected [**5a**]. Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. The security of personal information is always important, but t it is more significant in some situations than in others, depending on such matters as confidentiality and sensitivity and the harm that might result from an unauthorised disclosure (e.g. information about health status, political ideas, sexual life).

High standards of security are, nevertheless, essential for all personal information. The nature of security used may take into account what is available technologically, the cost of implementation and the sensitivity of the data in question.

KEY POINTS

A minimum standard of security would include the following:

- **access to central IT servers to be restricted in a secure location to a limited number of staff with appropriate procedures for the accompaniment of any non-authorised staff;**
- **access to any personal data within an organisation to be restricted to authorised staff on a 'need-to-know' basis in accordance with a defined policy;**
- **access to computer systems should be password protected with other factors of authentication as appropriate to the sensitivity of the information;**
- **Definition of computer protection and of manual files to be kept hidden;**
- **back-up procedure in operation for computer held data, including off-site back-up;**
- **all reasonable measures to be taken to ensure that staff are made aware of the organisation's security measures, and comply with them;**
- **all waste papers, printouts, etc. have to be disposed carefully;**
- **a designated person should be responsible for security and for periodic reviews of the measures and practices in place.**

4. Rights of Data subject

"What do I have the right to be informed about?"

Data subject has the duty to be informed about:

- the identity of the controller and his representative, if any
- the purpose of the processing

c) any further information such as

- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
- the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary,
- having regard to the specific circumstances in which the data are collected,
- to guarantee fair processing in respect of the data subject [5b, 5c],

KEY POINTS

The controller is an entity either in the public or private sector which is responsible for processing personal data, for example, a medical practitioner, a company, a sports club, a public administration, etc.)

The controller has the duty

- **to ensure that personal's rights are observed (i.e. inform the person, give access to his/her data);**
- **to ensure that data are collected only for specified, explicit and legitimate purposes,**
- **to ensure that they are kept accurate and up to date and for no longer than is necessary;**
- **to ensure that the criteria for making data-processing legitimate are observed, for example when a person gives his/her consent**
- **to obtain his/her consent**
- **to guarantee the confidentiality of the processing;**
- **to guarantee the security of the processing.**

"What do I have the right of accessing?"

The right of access is usually exercised by the representative of the child, but always in the interest of the child.

Every data subject have the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:
- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning the patient at least in the case of the automated decisions referred in Article 15 [**5**];

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

"What do I have the right of objecting?"
The data subject has the right**:

(a) to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

KEY POINTS

When personal data are processed the person has

- **the right to be informed that his/her personal data is being processed in a clear and understandable language;**
- **the right to have access to his/her own data;**
- **the right to rectify any wrong or incomplete information;**
- **the right, in some cases, to object to the processing on legitimate grounds;**
- **the right not to be subjected to an automated decision intended to evaluate certain personal aspects relating to the patient, such as performance at work, creditworthiness, reliability, and conduct;**
- **the right to receive compensation from the data controller for any damage the patient suffer, etc**

The Eight Rules of Data Protection
Investigator must...
1. Obtain and process information fairly
2. Keep it only for one or more specified, explicit and lawful purposes
3. Use and disclose it only in ways compatible with these purposes
4. Keep it safe and secure

5. Keep it accurate, complete and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it for no longer than is necessary for the purpose or purposes
8. Give a copy of his/her personal data to an individual, on request

DEFINITIONS

Age classification of paediatric patients: According to ICH Topic E 11,

• preterm newborn infants
• term newborn infants (0 to 27 days)
• infants and toddlers (28 days to 23 months)
• children (2 to 11 years)
• adolescents (12 to 16-18 years (dependent on region))

According to the Directive 95/46/EC:

(a) "personal data": any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity**;**

- Data means information in a form which can be processed. It includes both automated data and manual data.

- Automated data means, broadly speaking, any information on computer, or information recorded with the intention of putting it on computer**.**

- Manual data: information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system.

- Data Subject is an individual who is the subject of personal data**.**

- Sensitive personal data relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

(b) "processing of personal data" ("processing"): any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) "personal data filing system" ("filing system"): any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

Relevant filing system: any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information is accessible.

(d) "controller": the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law**;**

- Data Controllers can be either legal entities such as companies, Government, Departments or voluntary organisations, or they can be individuals such as G.P.'s, pharmacists or sole traders.

- Data Controllers are those who, either alone or with others, control the contents and use of personal data.

(e) "processor": a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

Data Processor is a person who processes personal data on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of his/her employment. Again individuals such as G.P.'s, pharmacists or sole traders are considered to be legal entities.

(h) "the data subject's consent": any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

* Adolescent aged 16 to 18 is no longer a minor as defined in national law, or is an "emancipated minor", then written informed consent is required from these individuals as for any adult capable of giving consent. (ICH E11)

** excluding the cases for which processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection.

References

1. Rocchi et al. *The european paediatric legislation:benefits and perspectives*. Italian Journal of Pediatrics 2010, 36:56.
2. Burns JP. *Research in children*. Crit Care Med. 2003;31(suppl):S131-S136.
3. Philippe Auby. *Pharmaceutical research in paediatric populations and the new EU Paediatric Legislation: an industry perspective* Child and Adolescent Psychiatry and Mental Health 2008, 2:38.
4. *Regulation (EC) No 1901/2006 of the European Parliament and of the Council of 12 December 2006 on medicinal products for paediatric use and amending Regulation (EEC) No 1768/92, Directive 2001/20/EC, Directive 2001/83/EC and Regulation (EC) No 726/2004*
5. *Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data*

a art.17
b art. 10
c. art. 11