Grant agreement no. 211714

neuGRID

A GRID-BASED e-INFRASTRUCTURE FOR DATA ARCHIVING/ COMMUNICATION AND COMPUTATIONALLY INTENSIVE APPLICATIONS IN THE MEDICAL SCIENCES

Combination of Collaborative Project and Coordination and Support Action

Objective INFRA-2007-1.2.2 - Deployment of e-Infrastructures for scientific communities

Deliverable reference number and title: D2.3 PROTOCOL FOR ENSURING DATA PROTECTION/SAFETY IN neuGRID

Due date of deliverable: month 12

Actual submission date: January 30th 2009

Start date of project: February 1st 2008 Duration: 36 months

Organisation name of lead contractor for this deliverable: PROVINCIA LOMBARDO-VENETA - ORDINE OSPEDALIERO DI SAN GIOVANNI DI DIO FATEBENEFRATELLI

Revision: Version 1

Project co-funded by the European Commission within the Seventh Framework Programme (2007-2013)		
Dissemination Level		
PU	Public	PU
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Table of contents

Executive summary

The present deliverable provides for a specific and unified data protection protocol for neuGRID.
The protocol is based on a revision of privacy and data protection issues in the European context with specific regard to Directive 95/46/EC and its implementation by Member States (D2.1 *Review document on data protection (legal and procedural issues)*). The data protection protocol for neuGRID is built on the following key points: 1) data are considered as personal data when the data subject may be identifiable; 2) specific informed consent of the person concerned is always required for the processing of sensitive data; 3) secondary use of data for scientific research purposes exempts from the duty to inform data subject only if the use of data is compatible with the original purpose, the data are anonymized and the provision of information is impossible or impracticable.
The aforementioned key points have been taken into consideration with reference to two major scenarios: a) clinical data and images are collected from subjects specifically enrolled to be entered in neuGRID project; b) clinical data and images were previously collected in different research projects and have been used, processed or communicated in or through the neuGRID e-infrastructure.

1 Introduction

The present deliverable provides for a specific and unified data protection protocol for neuGRID. The importance of the matter is based on the acknowledgment of privacy as a fundamental human right, as stated by all major international treaties and agreements on human rights. The protection of privacy of personal medical data is important in any use of such data, but it becomes even more important in the context of research where the right to privacy should not be overcome by other interests. In context of healthgrids, the protection of privacy deserves specific regard for the technical specificity of the tool. In fact, the distributed nature of grids and the many players involved in grid computing could make the control of sensitive information more difficult. For these reasons, as early as the planning phase of the project, the consortium decided to develop a specific and unified protocol for privacy and data protection. In order to develop the protocol, a review of the European and Member States regulations as well as of previous results of European projects on data protection had to be performed (D2.1 *Review document on data protection (legal and procedural issues)*. In that review we analyzed the *Directive 95/46/EC of the European Parliament and of the Council of 24.10.95 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* that sets a milestone in the European history of the protection of personal data and its implementation in Member States, with particular regard to the provisions related to biomedical research. As we pointed out in the deliverable D2.1, Directive 95/46/EC has not been implemented uniformly in all Member States' legislations. Furthermore, the Directive itself includes a number of broadly formulated provisions that, either explicitly or implicitly, leave Member States considerable latitude in its adoption into national legislation. Anyway, differences among national legislations on data protection are not such as to prevent the possibility of a common protocol on privacy issues.

The data protection protocol for neuGRID is built on the following key points: 1) data are considered as personal data when the data subject may be identifiable; 2) specific informed consent of the person concerned is always required for the processing of sensitive data; 3) secondary use of data for scientific research purposes exempts from the duty to inform data subject only if the use of data is compatible with the original purpose, the data are anonymized and the provision of information is impossible or impracticable.
The aforementioned key points have been taken into consideration with reference to two major scenarios: a) clinical data and images are collected from subjects specifically enrolled to be

entered in neuGRID project; b) clinical data and images were previously collected in different research projects and have been used, processed or communicated in or through the neuGRID e-infrastructure.
In the implementation of the data protection protocol, any additional requirement imposed by the national law in order to legitimate the processing of sensitive data, such the notification to the national supervisory authority, as well as local regulations requirements should be met by the local centres.
The final users will sign the data use agreement that will be elaborated by the consortium in which they commit themselves to not attempt to establish any individual identity.

A data protection framework depends ultimately on the security of the infrastructure (hardware and software) on which it is implemented. The project is implementing security as part of its technical development; the security design is therefore reported in that context.

2 Methodological approach

In the development of the data protection protocol for neuGRID we first started from the revision of the European legal framework on data protection in which Directive 95/46/EC and its implementation in Member States was analysed, with particular regard to the provisions related to biomedical research.
In the absence of specific rules for the anonymization process n the European context, we have taken into consideration the USA HIPAA Privacy Rule (45 CFR Parts 160, 162 and 164) provisions.
ADNI - Alzheimer's Disease Neuroimaging Initiative – being the most important data set in the world for clinical data and images in the field of Alzheimer disease, we have considered the ADNI policy related to data protection. We have taken into consideration also the BIRN - Biomedical Informatics Research Network - policy.
A search in Pub Med has been performed specifically to know the state of the art related to anonymization of images and defacing, using the following key words: brain images, privacy, data protection, DICOM, de-facing.
The ethics committees of the centres involved in neuGRID project have been asked for any specific local rules on data protection.
The neuGRID data protection protocol will be submitted to the Independent Ethics Committee set up for neuGRID as well as to the Ethics Committees of neuGRID partners.
Any comments or suggestions from the Ethics Committees will be taken into account and the present deliverable will be updated in accordance with them.

3 Data Protection Requirements: Analysis and Consequences

3.1 Data: definitions

This deliverable concerns itself with **personal data**, always considered to be held in a computer based system or in some other electronic form (e.g. stored on a CD). Personal data is data that relates to a particular identifiable individual. An individual's **right to privacy** is considered a fundamental human right and entails their ability to decide who may collect, view, hold, treat, transform, transmit, archive or otherwise use their personal data (in short **to process** their data; this term encompasses all other data-related activities in legal language).

It is sometimes necessary to use the verb "to process" in a non-legal, narrow sense: to hold temporarily, treat, transform and then remove the said data from the system. Its narrow use will be clearly signalled in the text.

There are many techniques to assist in **data protection**, the principle that it is incumbent upon the data processor (in the broad sense above) to ensure that personal data is not disclosed, whether accidentally or deliberately, in good faith or maliciously. These include:

- **encryption** of the data: transformation of the data according to a well understood, secure cryptographic protocol to an agreed standard; the standard normally specifies the effort necessary to break the encryption and this should normally be beyond the means of any likely attacker.
- **anonymization** of the data: the removal of any information from a record that may potentially identify the patient in such a way that even the processor that anonymized the data can no longer identify the patient.
- **pseudonymization** of the data: encryption of the identifying entries in the record (such as hospital number, name, date of birth, etc) in such a way that only the possessor of a particular private cryptographic key may be able to reverse the process.

Anonymization and pseudonymization cannot be guaranteed to be perfect. There is a sophisticated body of work which shows that the effort the would-be hacker is willing to make also determines how safe the anonymization or pseudonymization process is. Use of terms like **complete** or **full anonymization** should be interpreted as meaning anonymization as above, with all conceivably identifying items of information excluded from the record.

The processes of anonymization and pseudonymization are occasionally referred to as **de-identification**. When it is reversible, the reverse process is termed **re-identification**. De-identification is particularly appropriate to data that includes imaging of the head, where the face needs to be disguised in some way to prevent recognition; this is referred to as **de-facing** (spelt with a hyphen to differentiate it from 'defacing' = maliciously destroying by overwriting).

3.2 Sources of data

There are two distinct sources of data for the neuGRID project and a third possibility for neuGRID processing:

- (A) data that has been collected by neuGRID subject to all relevant regulatory frameworks, ethical clearance and informed consent.

- (B1) data that has been legitimately collected in another project for the purposes of research and which may be legitimately made available to neuGRID for further processing (in the broad sense above).

- (B2) data that has been collected in other, essentially independent, projects but subject to the neuGRID protocol, so that functionality offered by neuGRID may be used to process the data (in the narrow sense of 'process') but not to store it in neuGRID.

3.3 Data protection protocol. Key points: anonymous data, informed consent, secondary use

The three key points that we have taken into consideration in the development of neuGRID Data protection protocol relate to: - the notion of anonymous data; - the requirement of subjects' informed consent; - the secondary use of data.

3.3.1. ***The notion of anonymous data***

Directive 95/46/EC does not clarify what "anonymous data" signifies, so its meaning has to be inferred from certain provisions of the Directive starting from the notion of "personal data" as opposite to "anonymous data".
First of all Article 2(a) of the Directive defines as personal data "any information relating to an identified or identifiable natural person; 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".
Moreover Recital 26 states that " ...to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principle of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable...".
Beside the aforementioned Recital 26, the only reference to anonymization contained in the Directive is Article 6 affirming that "personal data must be kept in a form which permits identification of data subject for no longer than is necessary for the purposes for which data were collected or for which they are further processed".
The national laws differ in the implementation of the definition of personal data: while some States (i.e. Belgium; Greece; Italy; Luxembourg; Portugal; Sweden) have used the same or similar wording to the Directive without reference to the reasonable means of Recital 26, other States (i.e. Czech Republic; France; Germany) have introduced a limit on indirect identification as stated in Recital 26. Finally, certain States (i.e. Austria; Ireland; the Netherlands; United Kingdom) have used different wording to the Directive giving their own interpretation of Article 2(a) and Recital 26.
In accordance with the strictest interpretation of the Directive, data are considered as personal data while someone is able to identify the data subject (directly or indirectly), contrarily data should be considered completely anonymous only when nobody can identify the data subject. To realize that, any elements which permit subject identification and any link to the subject must be removed.

In the neuGRID protocol for data protection we have adopted a "relative" notion of anonymous data: data must be fully anonymous for the final users of the grid, and, as far as it is technically possible, for the researchers of the coordinator laboratories (core labs) involved in the control of data quality. On the contrary, the centre that first collected the data needs to have the possibility to re-identify the subjects, if this is in the subjects' best interest, and the subject needs to maintain the possibility to withdraw from the projects.
This solution resulted from the consideration of different interests of the research subjects: the interest to privacy, the interest to health, the interest to withdraw from the project. In fact, if a full anonymity is the preferable solution to ensure the maximum degree of data subject privacy because no link with the subjects is maintained, the removal of any link between data and the subject concerned prevent both the possibility to inform the data subjects about research results that can be in the subjects' health interest, and the subjects' possibility to withdraw consent.

3.3.2. ***The requirement of subjects' informed consent***

The requirement of informed consent is of capital importance in order to protect the fundamental rights of a subject in the context of medical treatment and research. From an ethical and legal point of view informed consent protects subjects and their fundamental rights to integrity and self-determination. Consent is the *condicio sine qua non* not only for the subject inclusion in a research project but also in order to legitimate the processing of personal data of the subject concerned.
Since the aim of the present deliverable is to draft a protocol for data protection in neuGRID hereinafter the focus will be on consent for the processing of data rather than on consent for the enrolment in a research project.
Directive 95/46/EC detects in consent the main criterion to permit the processing of sensitive data (Article 8.2 (a)). The explicit consent of the data subject - meant as any freely given, specific and

informed indication of wishes by which the data subject signifies his/her agreement to the processing of his/her data – removes the general prohibition to process sensitive data stated in the article 8.1 of the Directive.
Informed consent is not the unique condition that is able to overrule the ban to process sensitive data: in some national implementation of the Directive 95/46/EC, conditions other than informed consent permit the processing of sensitive data. In particular, in some cases (Belgium; Luxembourg; Norway; Sweden; United Kingdom) scientific research is considered to be in "substantial public interest", in other cases (Austria; Cyprus; Denmark; Finland; France; Germany; Poland) the national law of implementation provides for a specific exemption to the ban of processing sensitive data based on research purposes.
However these exemptions other than consent are not shared with all Member States and in the context of a uniform neuGRID protocol for data protection we have to find a common denominator ensuring the lawfulness of data processing. In this context, the informed consent of the data subject represents the best and safest solution in order to legitimate the processing of sensitive data.
According to Data Protection Directive, consent must be: explicit (Article 8.2(a)), freely given (without duress), for a specific purpose (generic consent in not valid) and informed (Article 2(h)).
There is little in Directive 95/46/EC as far as the form of consent is concerned. Article 8.2 simply states that the prohibition to process sensitive data may be removed with the data subject's explicit consent, ruling out the possibility of an implied or presumed consent. However, Directive 95/46/EC does not clarify which form the explicit consent should take. So, it is necessary to look at the requirements provided by the national legislators in the Directive implementation laws. There is no general consensus among Member States on the topic: the majority of them reproduce the Directive provision without specifying a particular form for the expression of consent. However, in certain States (i.e. Belgium, France, Germany, Italy, Spain) a written consent is expressly required to process sensitive data.

In the neuGRID protocol for data protection, informed consent for the processing of personal data should be given in a written form, in order to comply with the strictest legal and ethical requirements.
Research subjects have the right to refuse the processing of their data; anyway, subjects need to be aware that their participation in the research project is possible only if they agree with the processing of their personal data.
Research subjects have also the right to withdraw their consent in any time.
If subjects revoke their consent any further processing of their data has to be considered unlawful, therefore their data and images must be removed from neuGRID data set as soon as possible.
A temporary re-identification, that is possible only if data are pseudonymized, will be put in place in order to allow the cancellation of the data. The right to refuse the data processing and the right to withdraw should be clear in the informed consent form.

3.3.3. ***The secondary use of data***

According to Article 6(b) of the Directive 95/46/EC "data must be collected for a specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes". Moreover the same Article 6(b) states that "further processing of data for [..] scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards".
Therefore there is an assumption of compatibility between the original (collection) purpose and further scientific purposes. However, according to the Article 11.1 of the Directive, data subjects must be informed of the secondary use of their data: in particular, they should be informed about the identity of the controller and the purpose of the processing.

This duty of information can be lift only if the provision of this information is impossible or would involve a disproportionate effort. In these cases Member States shall provide appropriate safeguards (Article 11.2)

In the neuGRID data protection protocol, in case of secondary use of clinical data and images, subjects need to be re-contacted and asked for their informed consent. A secondary use of data for scientific research purposes exempts from the duty to inform data subject only if all the following conditions are met:

- the use of data is compatible with the original purpose;
- the provision of information is impossible or impracticable; and
- the data are anonymized.

The compatibility of the secondary use and the impossibility or impracticability of providing information to the subjects must be evaluated case by case.

3.4 Data protection protocol. Two possible scenarios

It is possible to foresee two main scenarios for the neuGRID e-infrastructure:

A. clinical data and images are collected from subjects specifically enrolled to be entered in the neuGRID project;
B. clinical data and images were previously collected in different research projects and are used in the neuGRID e-infrastructure.

3.4.1 ***Scenario A***

Clinical data and images are collected from subjects specifically enrolled to be entered in neuGRID project: the following requirements on data anonymization and informed consent must be meet.

3.4.1.1 Anonymization procedure

In order to reach data anonymization, The Health Insurance Portability and Accountability Act (HIPAA, 1996) refers to two approaches to the de-identification: de-identification to a statistical standard; and de-identification by removal of 18 specific identifiers.
For reason of feasibility in the neuGRID project we adopt the removal of the identifiers. In the selection of the identifiers that need to be removed we aim to balance between guarding patient confidentiality and considering the needs of research which is performed to achieve results that will be beneficial to the medical community and the humankind. The suggested list results from the consideration of the HIPAA list[1] of identifiers that must be removed, revised to guarantee the research quality, in particular at the point C) related to "elements of dates".

[1] The HIPAA list of identifiers is the following: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000. (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses; (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers,

Since from MR DICOM images of the brain it is possible through a rendering of images themselves discover the biometric features of the subject concerned and potentially determine his/her identity, the scrambling of the data subject face will be performed for ensuring a suitable protection of data subjects privacy.
Because we work in a research context and not in a clinical one, since the very beginning of the data collection, the same way of anonymization can be put in place in all centres that take part in the project, unless this is not be possible for strictly technical reasons.

In order to anonymize clinical data and images, the following process should be put in place at the collecting centres level and at the core labs level. With regard to the collecting centres level, we can only strongly suggest guidelines that should be implemented, but this part of the anonymization process doesn't pertain directly to the neuGRID consortium.

1. Collecting centres level:
   a. first anonymization of data subjects through:
   i. For the clinical data: removal of all identifiers listed below;
   ii. For the images:
   - DICOM headers: removal of the same identifiers removed for clinical data
   - Structural images: de-facing of the images aimed to avoid the recover of subjects' face and potentially determine their identity.

   b. first coding ;
   c. transmission of clinical data and images to one the core labs preferably through CD, since the use of CD is more safe than web transmission.

2. Core labs level:
   a. Check of the anonymization procedure performed in the collecting centre;
   b. Implementation of the anonymization process, in case of incorrect/incomplete anonymization procedure:
   c. Second coding.

List of the identifiers to be removed:
(A) Names;
(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes;
(C) All elements of dates (except year) for dates directly related to an individual excluding: - birth date (month and year admitted); - exams/visits date (day, month and year admitted); - date of death (month and year admitted);
(D) Telephone numbers;
(E) Fax numbers;
(F) Electronic mail addresses;
(G) Social security numbers;
(H) Medical record numbers;
(I) Health plan beneficiary numbers;
(J) Account numbers;
(K) Certificate/license numbers;
(L) Vehicle identifiers and serial numbers, including license plate numbers;
(M) Device identifiers and serial numbers;
(N) Web Universal Resource Locators (URLs);
(O) Internet Protocol (IP) addresses;
(P) Biometric identifiers, including finger and voice prints;

---

including finger and voice prints; (Q) Full face photographic images and any comparable images; and (R) Any other unique identifying number, characteristic, or code.

(Q) Full face photographic images and any comparable images; and
(R) Any other unique identifying number, characteristic, or code.

The list of identifiers to be removed are mandatory only for data regarding research subjects.

3.4.1.2 Informed consent

Subjects' consent for the processing of sensitive data must be explicit and given in a written form.
In the informed consent sheet for the participation in the clinical trial, the section related to the processing of data should be clearly separate from the information about the clinical trial procedure, even if the subjects needs to be aware that the participation in the research project is possible only if they agree with the processing of their personal data. Moreover the part of the informed consent form in which the subjects are asked to sign should repeat clearly that the consent is given both for taking part to the clinical trial and for the processing of sensitive data. In order to make clear the double consent, it would be preferable to have two separate signatures.
With regard to the processing of personal data, subjects must be informed of:

- the purpose of the data processing, including the specificities of the GRID (this information corresponds to the clear and full information about the clinical trial and the neuGRID project);
- the identity of the controller and of his/her representative, if any;
- the procedures adopted in order to guarantee anonymity;
- the possibility to withdraw their consent in any time asking for the cancellation of their data.

In particular the subjects should be informed that: - the link between data and subject identity is maintained only in the collecting centre, with the aim to ensure the possibility to re-contact the subjects, if it is in their best interest, and the aim to give the subjects the possibility to withdraw; - the data are subjected to a double-coding process, the first in the collecting centre and the second in one of the neuGRID core labs; - every technical possibility is put in place for ensuring the full anonymity of the data subjects for the final users.
The informed consent should make reference to the national data protection law and to specific local rules, if any.
The information sheet and the informed consent form, as well as the research project protocol, must be approved by competent Independent Ethics Committees.

3.4.2 ***Scenario B***

Clinical data and images were previously collected in different research projects and are used in the neuGRID e-infrastructure, with two different possibilities:

1. the data are collected in neuGRID
2. the data are used, but not collected, in neuGRID

In this scenario, informed consent and anonymization issues have already been handled in some way in the original research protocols.

3.4.2.1. ***Scenario B.1***

The data collected in previous research protocols are transferred to neuGRID.
Before the inclusion of clinical data and images in neuGRID e-infrastructure it is necessary to investigate whether the original protocol and the subjects' informed consent give this possibility.
It is possible to define three different hypotheses:

i) previous research protocol gives the possibility that data collected be included in other datasets/neuGRID;
ii) previous research protocol rules out the possibility that data collected be included in other datasets/neuGRID;

iii) previous research protocol does not take into account the possibility that data collected be included in other datasets/neuGRID

In case i) the collection of the data in neuGRID is possible
In case ii) the collection of data in neuGRID is not possible
In case iii) the collection of data in neuGRID is possible under some conditions.

3.4.2.1.1. Informed consent

In case i) the subjects have already expressed their consent to the collection of the data in other data sets/ grid and the collection of the data in neuGRID is possible.
In case iii) the persons concerned have not expressed their informed consent because the original research protocol did not take into consideration the possibility that data collected might be included in other datasets. In this case it is possible to collect data in neuGRID with the consent of the person concerned who should be informed at least about: - the new purpose of the processing (i.e. inclusion in neuGRID); and – the identity of the controller or his/her representative, if any.
Taking into consideration that, in the present case, the secondary use of data is for scientific research purposes, it is possible to foresee exemptions to the duty to inform data subject if the use of data is compatible with the original purpose and the provision of information is impossible or impracticable. Moreover, the data must be anonymous.
Maximum effort should be put in place in order to re-contact the subjects; mere difficulty is not enough to exempt the controller from the duty to inform.
The compatibility of the secondary use, the impossibility and impracticability of providing information to the subjects need to be evaluated case by case by the ethics committees of the collecting centres.

3.4.2.1.2 Anonymization procedure

To be included in neuGRID e-infrastructure clinical data and images should be anonymized according to the procedure defined for scenario A (see par. 3.4.1.1). The collecting centre has the task to implement, as far as possible, the first anonymization if incomplete/incorrect when compared to the neuGRID standard. At the level of the core labs the following operations are required:

a. Check of the anonymization procedure performed in the collecting centre
b. Implementation of the anonymization process, in case of incorrect or incomplete anonymization procedure
c. Second coding.

3.4.2.2. ***Scenario B.2***

The provision is to give the final users the possibility to work on data already collected in other data sets using the neuGRID computational facilities; clinical data and images are not collected/archived in neuGRID but only temporary used in the grid. It is assumed that secondary use issues have already been addressed.
The final researchers interested in using neuGRID with clinical data and images collected in other data sets, need to follow the rules for the access to the data sets established by the data sets' owner. After obtaining the authorization to the use of the dataset from the datasets owners, the final users can access neuGRID following the rules established by the neuGRID consortium in the user agreement.

3.4.2.2.1 Informed consent

The data set owner has the duty and responsibility to evaluate if the use of the clinical data in neuGRID is compatible with the informed consent expressed by the subjects.

3.4.2.2.2 Anonymization procedures

In case the original research protocol does not provide the same level of guarantee of data protection as neuGRID and does not provide for the de-facing in the anonymization procedures, neuGRID will provide for the removal of the identifiers listed in the neuGRID data protection protocol and will provide for the de-facing of the images that will be used in its grid.

3.5 Data protection protocol. Open issue: subjects' capacity to give informed consent

In the health field, informed consent is a fundamental ethical requirement in order to guarantee the principle of respect for the autonomy of human beings and to safeguard patients' right to self-determination. When treatment and research involve persons who may be cognitively impaired, such as those with Alzheimer's disease, competence assessment is an important task for physicians and researchers and, indeed, is subject to specific legislation in some EU member states.

In the development of a protocol for data protection, we are dealing specifically with informed consent to the processing of particularly sensitive personal data, and not with the more general issue of informed consent for participation in a clinical trial. Our suggestion is that in the evaluation of any given subject's competence to give consent to their enrolment in the clinical trial, researchers explore also the subject's understanding of the aspects related to the processing of clinical data. Nevertheless, the hypothesis is that subjects competent to give informed consent for the participation in the clinical trial are also competent to give consent for the processing of personal data. In case of subjects not fully competent to give informed consent, rigorous protective measures should be set up, conformant with local regulatory frameworks where applicable.

4 Conclusions

We have proposed a data protection protocol for neuGRID. The suggested protocol is set up in the context of European ethical and legal frameworks and takes into consideration both the possibility that data are collected from subjects specifically enrolled to be entered in neuGRID project and the possibility that data are already collected in other research protocols and datasets.