DATA SECURITY POLICY

The following safety measures are intended to guarantee the privacy, integrity and availability of data and the resilience of the informatics systems (analogical and digital). They consist of technologic, procedural and organizational procedures aimed to implement the appropriate level of security of the use of personal information. Following analyses of usage and the evaluation of its related risk, as established in art. 32 of GDPR, these technical and organizational measures are meant to reduce to the minimum the risks of:

- Removal or loss, also accidental, of the data;
- Non-authorized access;
- Usage not in accordance or not allowed by the purposes of the data collection;
- Modifications of data following not authorized or not compliant to the defined rules.

The data security is divided in three main areas: physical security, network security, and system security.
Physical security means the access and the physical protection of relevant structures relevant for data preservation and the safe maintenance of hardware and software.
Network security means the safeguard of systems, particularly those exposed to the internet and, therefore, to hacker attacks (implementation of network firewall and DMZ).
System security ensures the appropriate management of computers by users:

- Password management (how long and how frequently they have to be changed);
- Implementation of suitable control procedures of accesses;
- Implementation of adequate encryption procedures;
- Monitoring and filtering of transmitted data (personal filtrated data or just transfer of encrypted data);
- Safe removal of data, including tracing of produced alterations.

DOMAIN OF INTEREST/APPLICATION

This policy is applied to preservation and security of collected data in all Operative Unites/joint organizations of Istituto Neurologico “Carlo Besta”.

DATA SECURITY STANDARD

In compliance with the principles established in art. 35 of GDPR, Istituto Neurologico "Carlo Besta" exploits for data collection and preservation two platforms, REDCap and XNAT, that guarantee:

- Data and clinical metadata entry together with neuroimaging data such as magnetic resonance and CT scan;
- Creation of survey or online database with secure and certified access;
- Following authorization, the access to the two platforms by diverse researchers from different institutes;
- Control of users' activity and data manipulation;
- Advanced management and customization of users;
- User authentication with personal and complex passwords (it will be mandatory to change it after 3 months);
- Session expiration after 15 minutes of inactivity.

Additionally, further security measures will be adopted:

- Personal or confidential data will be encrypted;
- Servers will be protected by firewalls to prevent unauthorized accesses;
- The database will be accessible only from VPN-LAN-to-LAN;
- Server remote access will be guaranteed only using VPN connection, to enable encryption of sensitive data exchanged between the user and the server;
- Daily backups;
- Data collection will occur in an anonymized or pseudonymized approach;
- Only authorized staff will be able to access the data;
- The patient will have the possibility to require a copy of his/her data from the researchers.

The usage of personal data will take place both in automatized and manual format, respecting the adequate security measures described above and following the principles of lawfulness, objective limitation and minimization. These criteria will reduce to the indispensable the use of identifying data, to avoid their usage whenever each single case purpose can be achieved by the employment of anonymized data, or through the procedures that allow the identification of the patient only in case of necessity. In compliance with art. 28 and 29 of GDPR, only the authorized personnel can use the essential data to conduct the institutional activity. Please refer to what is specifically described in the sharing policy established by Istituto Neurologico "Carlo Besta".

MAIN RISKS ASSOCIATED TO DATA SECURITY

In compliance with the GDPR regulation, every research project considers the principles of minimization and limitation of data usage.
Since all the security measures described in the previous section are observed, we believe that the risks associated to the use of the system by authorized personnel is reduced to the minimum. Especially, our data collection system is verifiable in its entirety, safeguarding its traceability in every project phase.

The fulfillment of the research project requires that every partner works following the privacy principles pursuant to art. 25 clause 1 of GDPR, especially considering: the state of the art and the implementation costs, the nature, scope, context and purposes of the treatment, as well as the risks, having different probabilities and severities, for the rights and freedoms of the data subjects, posed by the treatment itself. In this sense, the principles of privacy by design establishes the obligation to adopt adequate security measures for the protection of personal data to guarantee data subjects.

The two main categories of security measures adopted to ensure a level of security against any risk can be identified in organizational measures and technical measures. These measures guarantee that, by default, only personal data which are necessary for each specific purpose of the processing are processed, with particular regard to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. Further, they ensure that, by default, personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

In order to observe the data security and to protect the rights and the freedom of the subjects, it is mandatory to verify that the owner of data treatment has the consent form from the patient himself/herself. Consent forms and Information Sheets have been tailored according to national laws and guidelines and to art. 4 of GDPR. Information Sheets for participants have been prepared, describing in a very simple and comprehensive language, the nature of the study, its purpose, the procedures involved, the expected duration, the potential risks and benefits involved and any discomfort it may entail. Each participant will be informed that participation in the study is voluntary, that he/she can withdraw from the study at any time and that withdrawal of consent will not affect her/his condition in any way.

In every research project, all partners are collectively committed to fulfil these technical and organizational measures in order to provide appropriate data protection.