Human Brain Project

THE MEDICAL INFORMATICS PLATFORM

MIP ETHICS AND LEGAL REQUIREMENTS

VERSION: 20.10_20200615

Document Control

Document Owner	MIP Deployment Team
Document Type	MIP Deployment Pack
Document Purpose	To provide information about ethical and legal issues concerning the MIP. Descriptions of GDPR, data privacy, annonymisation, etc

Date of update	Updated by (author name)	Changes Made and Brief Description	Version #
2020 05 05	Erika Borcel Alan Ames	Document created from template and copy of content from preexisting MIP Technical Specification Document & Installation & Set Up Project Charter(V01.00 2019 11 09)	
2020 05 12	Erika Borcel Alan Ames	Minor updates	V02.00
2020 06 15	Alan Ames	Footer logos added	V02.10

Table of Contents

1. Purpose

The present document outlines the Ethics and Legal requirements and responsibilities related to the deployment of the Medical Informatics Platform (MIP) into hospitals participating to the MIP network.

2. Introduction

MIP relies on citizens and patients allowing researcher to use their private personal medical data. MIP is a platform designed to enable large scale, privacy preserving data sharing for research purpose. It is the responsibility of the hospitals to make sure that their data subjects and patients have given their consent for the collection of the data. It is also the responsibility of the hospitals to ensure that this data has been properly pseudonymized / anonymized according to the standards and the recommendations of the MIP deployment team.

3. Data Collection

Data is not collected in the specific purpose of the MIP. It is collected in the course of the patient's health care or for research projects and can be further processed and shared using the MIP.

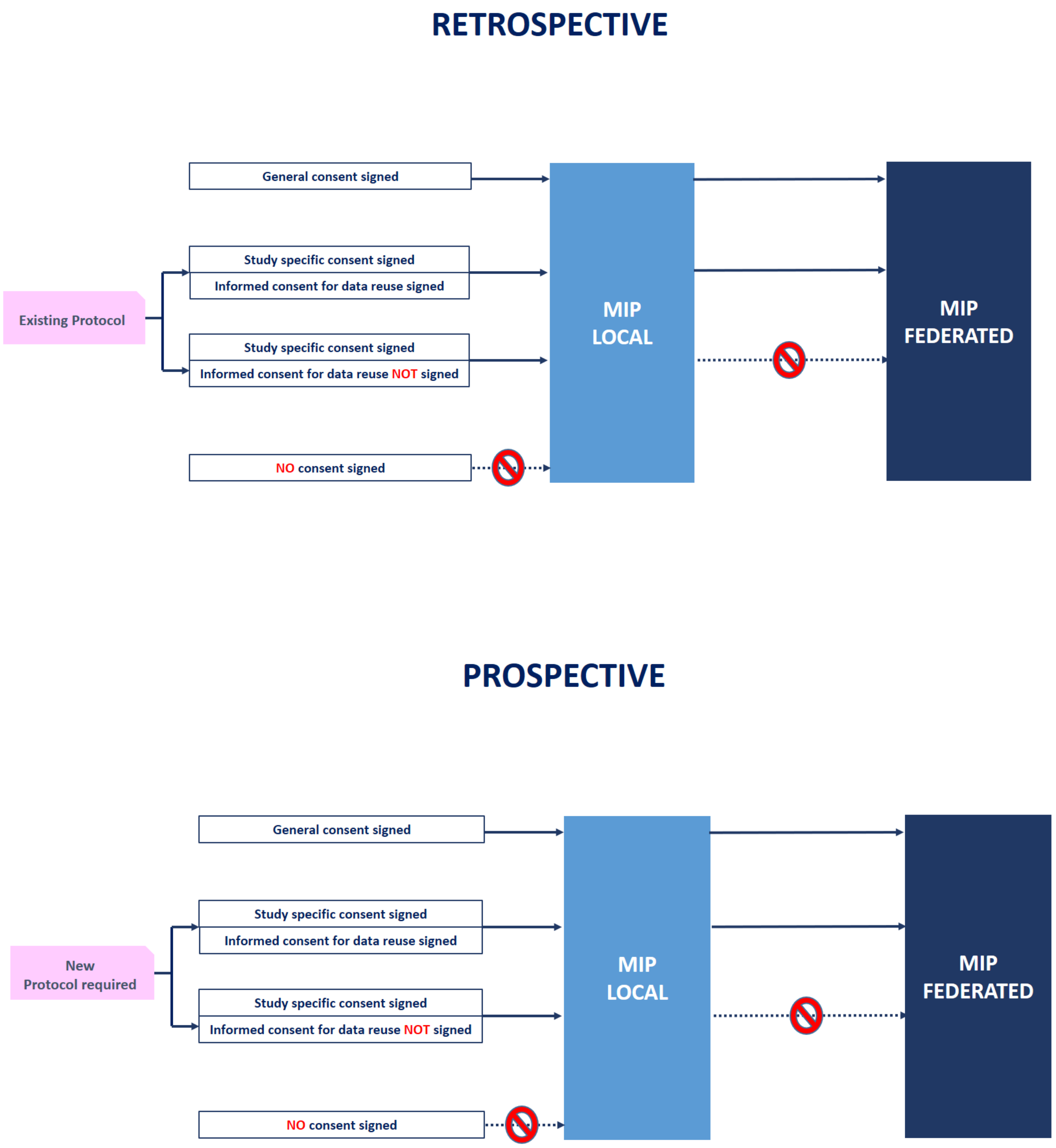
4. Consent

‘Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (see Article 7 of the GDPR);

In any case, hospitals are the only responsible to obtain informed consent from patients whose data are going to be analyzed. Withdrawal of consent also takes place at the partner’s local hospital.
A record of each consent is kept by the hospital to demonstrate that explicit consent has been obtained.
HBP research participation consent is not ‘bundled’ with medical treatment and participating hospitals make it clear to patients that the use of their medical data for the secondary research is optional

5. Usage of data in the MIP

Concerning entering retrospective data in the Federated MIP, there is no need for specific consent to reuse data if performing federated analysis was already defined as an objective within the frame of a clinical study. In all other cases, the signature of an informed consent allowing the re-use of patient’s data must be obtained (see Figure 1A).
In order to collect prospective data to be analysed using the Federated MIP, a new research protocol has to be submitted to the corresponding EC proposing to elaborate a multicentre cohort study justifying the use of the MIP as the tool needed to federate distributed cohorts (see Figure 1B).



RETROSPECTIVE

PROSPECTIVE

Existing Protocol
General consent signed
Study specific consent signed
Informed consent for data reuse signed
Study specific consent signed
Informed consent for data reuse NOT signed
NO consent signed
MIP LOCAL
MIP FEDERATED
New Protocol required
General consent signed
Study specific consent signed
Informed consent for data reuse signed
Study specific consent signed
Informed consent for data reuse NOT signed
NO consent signed
MIP LOCAL
MIP FEDERATED

Figure 1. Overview of the informed consent required to enter data in the MIP Local and Federated in Switzerland. A) Retrospective data; B) Prospective data.

6. Pseudoanonymisation - Anonymisation

Pseudonymization

> *According to GDPR Art. 4(c)*
> *'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;*

Anonymization

> *According to the Data Policy Manual of the HBP*
> *"Anonymous data: Information which does not relate to an identified or identifiable natural person." According to the Swiss Federal Act on research involving Human Beings, "Anonymised biological material and anonymised health-related data means biological material and health-related data which cannot (without disproportionate effort) be traced to a specific person;"*

Application of the GDPR

The GDPR only applies to personal data or information concerning an identified or identifiable natural per- son. If data are anonymised, it is no longer considered to be personal and is thus outside the scope of GDPR application. In other words, if data accessible in the MIP are anonymous, the GDPR does not apply and the data can be processed for research purposes without the restrictions of data protection law. However, given the difficulty in creating truly anonymous data, the bar for anonymisation has been set extremely high under EU data protection law.

Regardless of the technique applied (e.g. addition, permutation, differential privacy, aggregation, k-anonymity, l-diversity, t-closeness, etc.), three main questions should be considered:

1. Is it still possible to single out an individual?
2. Is it still possible to link records relating to an individual?
3. Can information be inferred concerning an individual?

On a general basis, data stored on the MIP local will be pseudonymised and is attributable to a natural person by the use of additional information, which is securely stored using both organizational and technical security measures.

Data on the MIP federated node will be anonymized. Taking into account all the means reasonably likely to be used for identification, data subjects cannot be identified through research data available at this level.

Data Providers are responsible for the pseudonymization and the anonymization of their data, based on the requirements provided by the MIP Deployment team.

All the identifiers are removed or coded and the patient record receives a unique encrypted identifier when it is stored on the MIP Local server. The look-up table is stored on a different server in the hospital level 3 "clinical area" which is not accessible from the outside.

A description of the anonymization process is available in the Data Processing User Guide.

7. Data Privacy Levels

Level 3 - Data stored in hospital's clinical data storage systems (EHR, PACS)

- Contains Personal Health Identifiers (PHI)
- Raw data, including full brain images that enable reconstructing the patient's face, diagnostics and longitudinal information with exact dates
- High risk of unauthorized identification
- General regulatory requirements: Cannot be shared publicly, must be protected from any un- authorized access.
- MIP policy: Such data are not accessible through the MIP

Level 2 - Pseudonymised data stored in MIP local

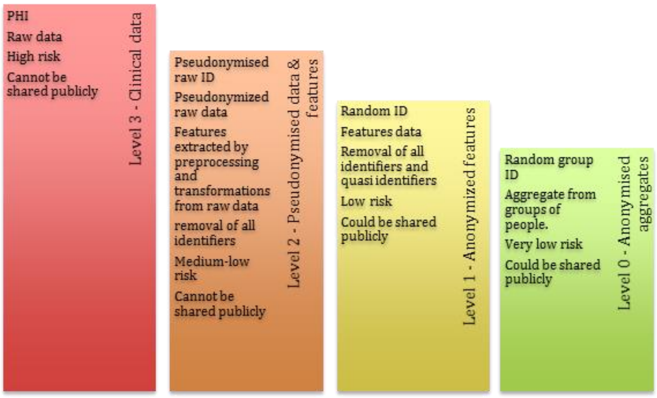
- No Personal Health Identifiers (PHI).
- Neuroimaging data are being processed in order to deface them in the case images are shared, or to extract features such as brain volumes.
- Medium to Low (from Raw to features) risk of unauthorized re-identification: identity can be recovered from a lookup table secured and password protected in a hospital server distinct from where the pseudonymised data are stored. In hospitals, the look-up table is stored on the level 3.
- General regulatory requirements: Can be shared by authorized investigators provided ethics approval and patient's informed consent whenever appropriate, but cannot be shared publicly and must be protected from any unauthorised access.
- MIP policy: Such data will be only accessible through the MIP local by the data provider and his local authorized staff.

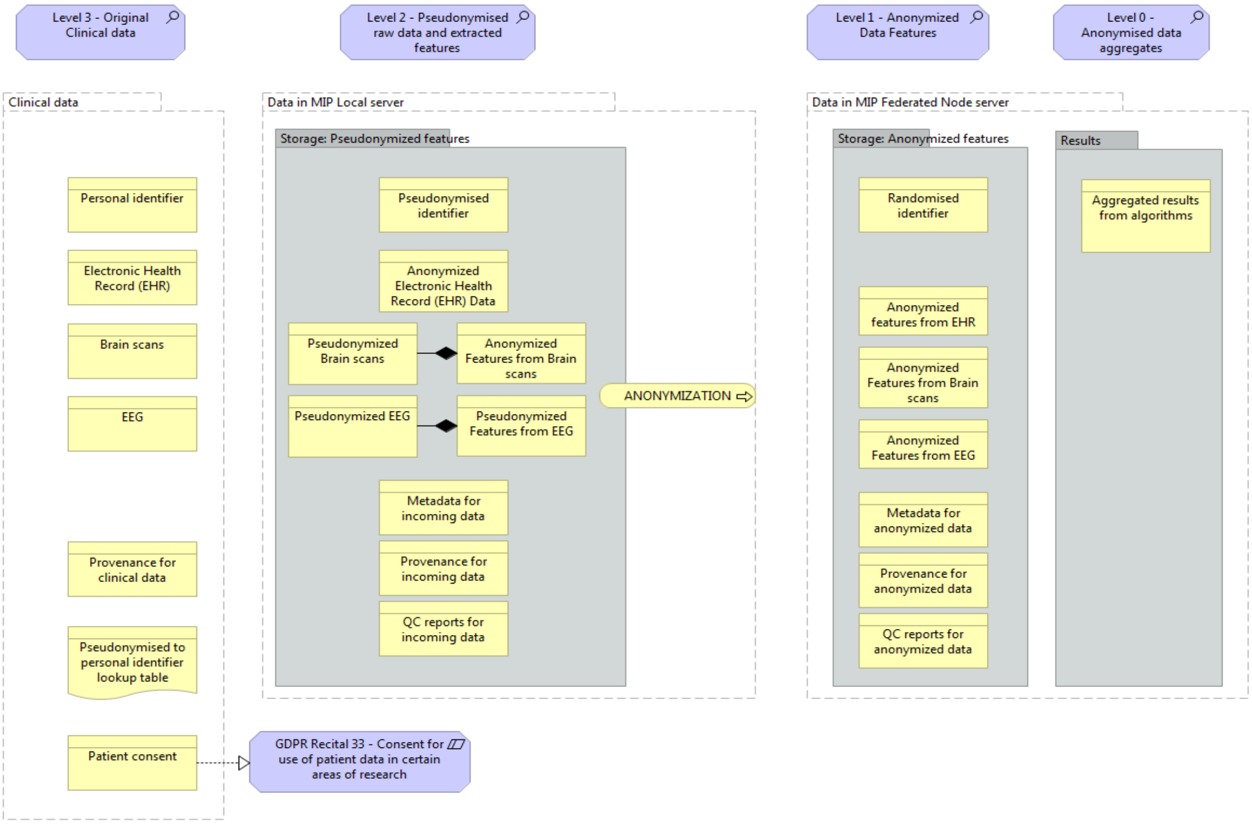
Level 1 - Anonymized data stored in MIP federate nodes

- Anonymization with no lookup table
- Only features data obtained after pre-processing of raw data (no available image that would allow reconstructing the face)
- Very low risk of unauthorized re-identification: identity cannot be recovered from a lookup table. Most features do not contain enough information to find directly or by cross-references the identity of an individual.
- General regulatory requirements: Can be shared by authorized investigators. Must be protected from any unauthorised access.
- **MIP policy: Such data cannot be explored at the individual level.** Data are made available for aggregated queries only within the MIP federate network to investigators authorized by the MIP Data Governance Steering Committee. Data will not be shared publicly, must be protected from any unauthorised access.

Level 0 - Anonymized data aggregates transmitted to MIP central

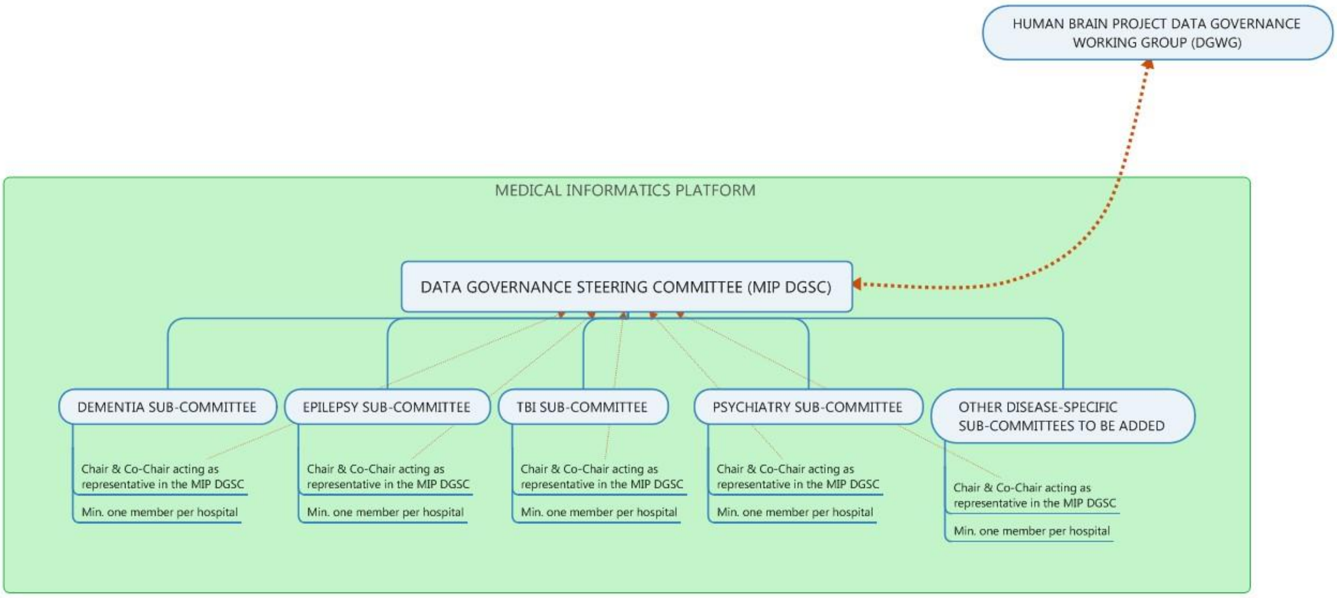
- Same as above with the following additional features:
- Only aggregated data (minimum values are set to the algorithms to ensure there is no singling out)
- MIP policy: Data will be made available for aggregated queries only to any MIP registered users
- No data storage happens at level 0, only per-call data queries of the results


PHI
Raw data
High risk
Cannot be shared publicly
Level 3 - Clinical data
Pseudonymised raw ID
Pseudonymized raw data
Features extracted by preprocessing and transformations from raw data
removal of all identifiers
Medium-low risk
Cannot be shared publicly
Level 2 - Pseudonymised data & features
Random ID
Features data
Removal of all identifiers and quasi identifiers
Low risk
Could be shared publicly
Level 1 - Anonymized features
Random group ID
Aggregate from groups of people.
Very low risk
Could be shared publicly
Level 0 - Anonymised aggregates


Level 3 - Original Clinical data
Level 2 - Pseudonymised raw data and extracted features
Level 1 - Anonymized Data Features
Level 0 - Anonymised data aggregates
Clinical data
Personal identifier
Electronic Health Record (EHR)
Brain scans
EEG
Provenance for clinical data
Pseudonymised to personal identifier lookup table
Patient consent
GDPR Recital 33 - Consent for use of patient data in certain areas of research
Data in MIP Local server
Storage: Pseudonymized features
Pseudonymised identifier
Anonymized Electronic Health Record (EHR) Data
Pseudonymized Brain scans
Anonymized Features from Brain scans
Pseudonymized EEG
Pseudonymized Features from EEG
Metadata for incoming data
Provenance for incoming data
QC reports for incoming data
ANONYMIZATION
Data in MIP Federated Node server
Storage: Anonymized features
Randomised identifier
Anonymized features from EHR
Anonymized Features from Brain scans
Anonymized Features from EEG
Metadata for anonymized data
Provenance for anonymized data
QC reports for anonymized data
Results
Aggregated results from algorithms

Please refer to the Executive Summary and the MIP Installation Prerequisites and Installation Guide for details of the MIP technical architecture to support these requirements.

8. Data Management Oversight & Governance


HUMAN BRAIN PROJECT DATA GOVERNANCE WORKING GROUP (DGWG)
MEDICAL INFORMATICS PLATFORM
DATA GOVERNANCE STEERING COMMITTEE (MIP DGSC)
DEMENTIA SUB-COMMITTEE
EPILEPSY SUB-COMMITTEE
TBI SUB-COMMITTEE
PSYCHIATRY SUB-COMMITTEE
OTHER DISEASE-SPECIFIC SUB-COMMITTEES TO BE ADDED
Chair & Co-Chair acting as representative in the MIP DGSC
Min. one member per hospital
Chair & Co-Chair acting as representative in the MIP DGSC
Min. one member per hospital
Chair & Co-Chair acting as representative in the MIP DGSC
Min. one member per hospital
Chair & Co-Chair acting as representative in the MIP DGSC
Min. one member per hospital
Chair & Co-Chair acting as representative in the MIP DGSC
Min. one member per hospital

9. Basis and Reference

- MIP is complying with the GDPR with special consideration to Privacy by Design and Privacy by Default. Legislation and Guidance
- REGULATION (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)- Applies from May 2018
- 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, OJ L 281, 31–50 (henceforth '95/46/EC' or 'the Directive').
- Working Party 29 'Opinion 216 05/2014 on Anonymisation Techniques' (2014) 5 ('WP29 216').
- Federal Act on Research involving Human Beings (Human Research Act, HRA) of 30 September 2011 (Status as of 1 January 2014)

10. Contact:

Erika BORCEL: erika.borcel@chuv.ch