Human Brain Project

THE MEDICAL INFORMATICS PLATFORM

MIP ETHICS AND LEGAL REQUIREMENTS

VERSION: JANUARY 2019

Human Brain Project

THE MEDICAL INFORMATICS PLATFORM

MIP DEPLOYMENT ETHICS AND LEGAL REQUIREMENTS

MIP LOCAL

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.

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.

Structure of the document

The following document presents information at two levels. Blue Text boxes are used to summarize and provide legal conclusions regarding application of the GDPR to the MIP.

The analysis and reasoning behind the highlighted text box conclusion is provided in more details with selected reference to the regulation. The intent of this structure is to provide an accessible or operational document while also providing expanded explanations for users requiring additional information.

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)

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. Storing the data for a longer period may require to submit an extension request with the competent body in the Member-State where the Data Provider is based. In such cases, a support from the CHUV-MIP Deployment team can be provided to streamline the process.

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;

Article 7 of the GDPR "Conditions for consent

1.Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2.If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3.The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4.When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Data Providers are responsible for obtaining the consent from their patients and / or data subject whenever appropriate.
Support and audit to make sure the informed consent form is compliant with the regulation can be provided by the MIP Deployment Team, as well as a template.

PSEUDONYMIZATION - ANONYMIZATION

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;"

The principles of data protection in GDPR does not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

Application of the GDPR

The GDPR only applies to personal data or information concerning an identified or identifiable natural person. 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.

To determine whether a person is identifiable, one must consider "all the means reasonably likely to be used,

such as singling out, either by the controller or by another person, to identify the natural person directly or indirectly." To make this determination, one must consider all "objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."
In making this determination, one must also consider the robustness of the anonymization techniques they apply and the potential for failure of those techniques. Like the Directive, the GDPR takes a 'risk-based approach', and obligations are scalable. Therefore, GDPR anonymization obligations require both interpretation and monitoring. Applying the GDPR to the MIP will thus remain an ongoing and continual process.
The main anonymisation techniques applied in data protection law are randomisation and generalisation. 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. Data stored on the MIP local (pseudonymised data) 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.

To ensure effective pseudonymization of the data, SP8 can provide technical support for the installation and configuration of the software used during SGA1 (FedEHR Gnubilla) and also the following guidelines for the pseudonymization of EHR data.

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 complete table of the recommended fields to modify- delete- mask is available in the Rules for Anonymization document, part of the Deployment Package.

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

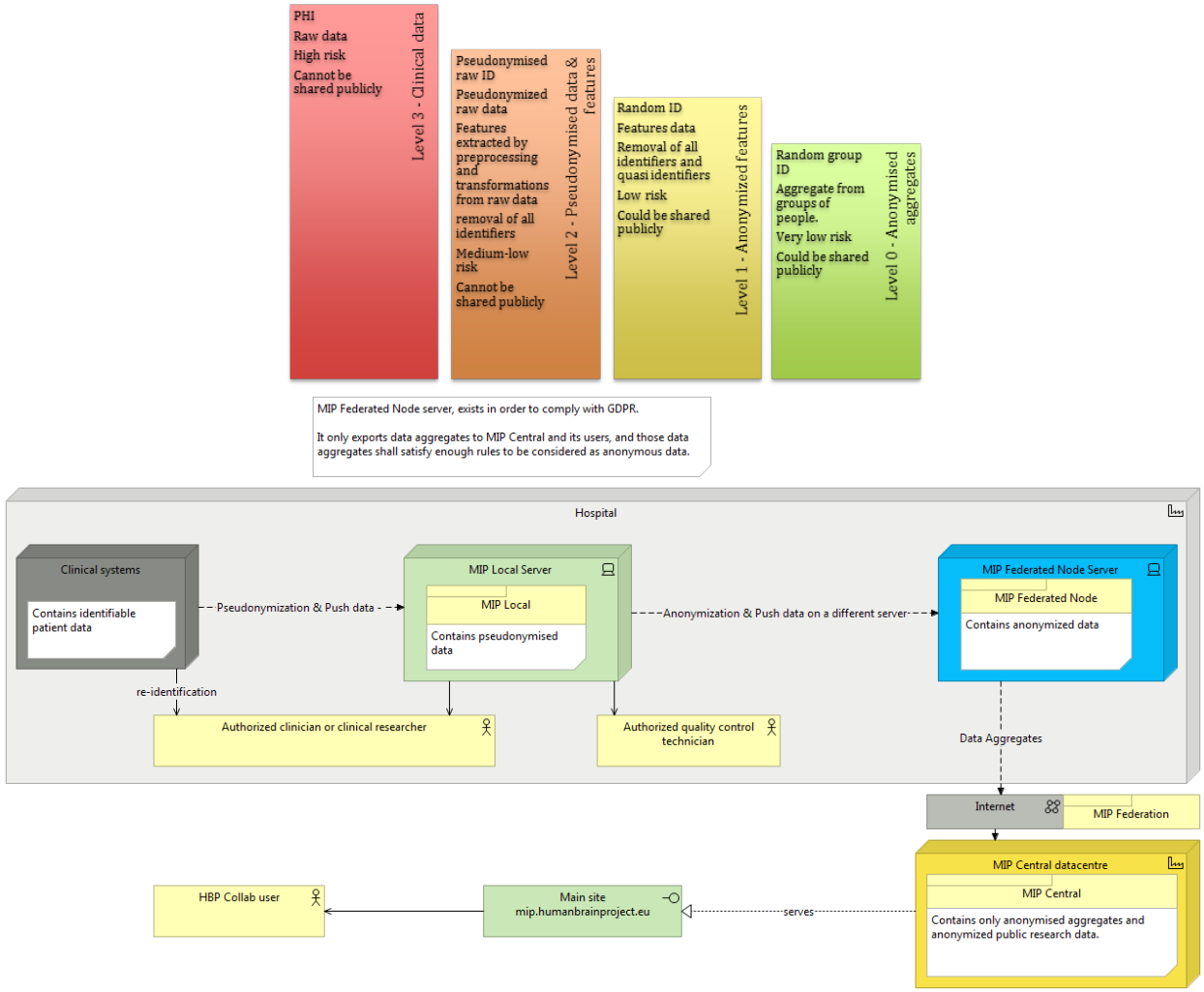
- Anonymization with no lookup table
- Only features data obtained after pre-processing of raw data (no available image that would allow reconstructing the face)
- Very low risk of unauthorized re-identification: identity cannot be recovered from a lookup table. Most features do not contain enough information 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. Will not be shared publicly, must be protected from any unauthorised access. An expert determination report assessing the strength of protection from re-identification should be provided for each dataset (similar to https://www.hipaajournal.com/de-identification-protected-health-information/)

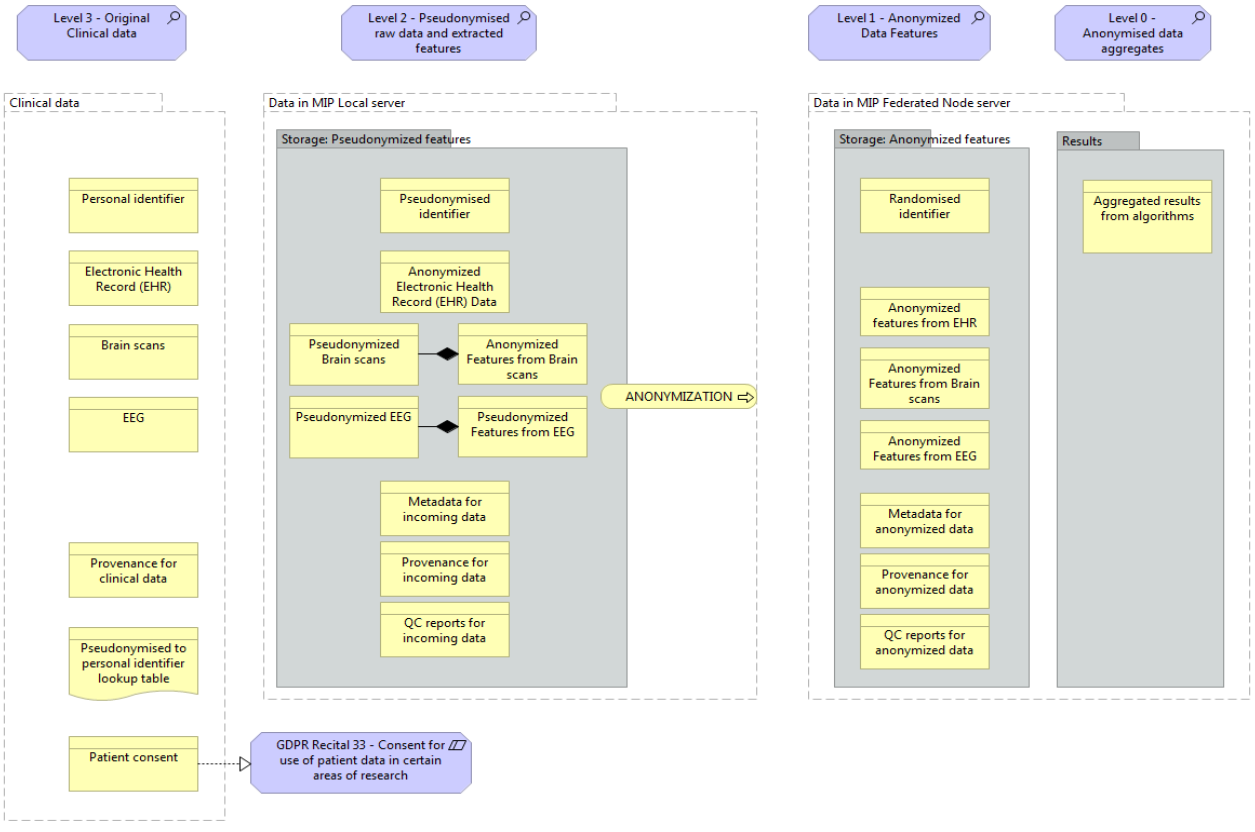
Level 0 - Anonymized data aggregates transmitted to MIP central

- 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.



To ensure data security, Data Providers shall allocate two different servers, one for the MIP Local and one for the MIP Federated Node. The MIP Federated Node Server will not contain any information allowing the reidentification of patients.

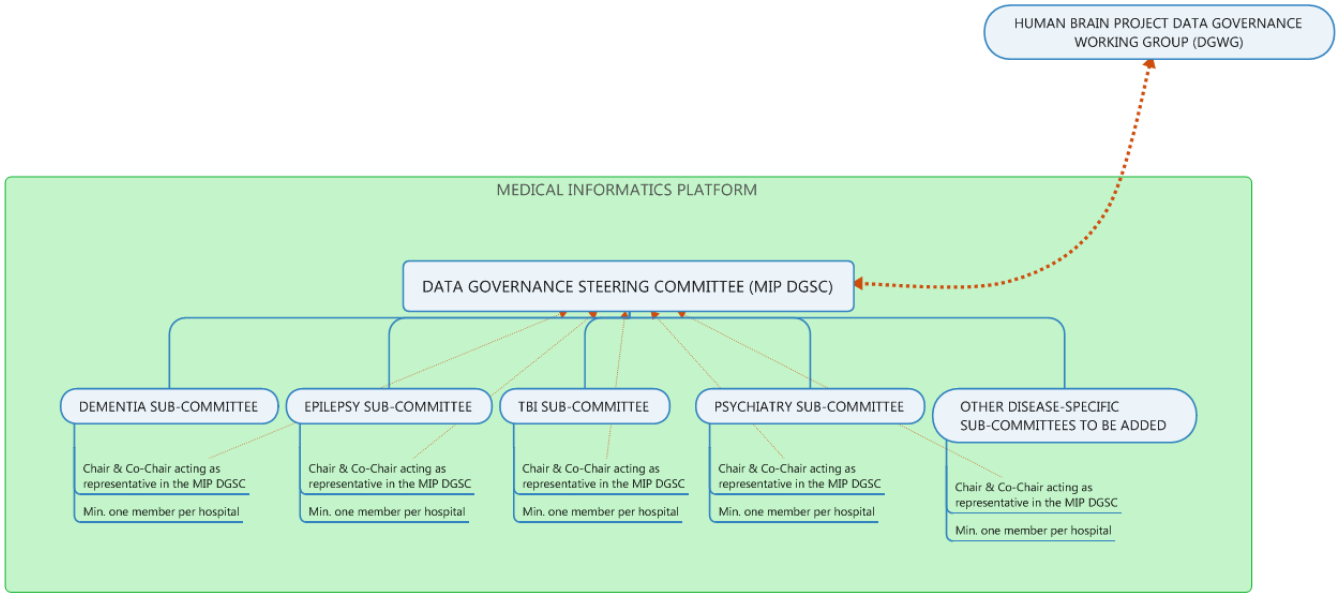


MIP Installation Agreement, MIP Data Sharing Agreement and Governance

As delineated in the Executive Summary of this Package, the Legal Entity representing the MIP is the CHUV, in Lausanne. Two agreements are signed between the CHUV and the Hospitals providing data.
- An Installation Agreement to cover the installation of the platform in the hospital, the responsibilities, the level of service provided by CHUV MIP Deployment Team and other relevant elements pertaining to the software installation
- A Data Sharing Agreement, covering the aspects of implementing and sharing the data at the MIP Federation Level.

Moreover, as stated in the Executive Summary, a MIP Data Governance Steering Commitee (MIP DGSC) is created to discuss all matters of Governance and produce the Charter for Data Sharing in the MIP and the Publication and Authorship Policy.

It is organized with 2 levels, a global MIP DGSC covering all the high level aspects, rules and guidelines, and Pathology-specific sub-committees to go deeper into each specific disease, as illustrated below.



Available Documentation

For in-depth documentation on compliance, ethics and governance issues, plsease contact Florent Gaillard.

CONTACT:

CHUV MIP Ethics and Governance Officer: Florent Gaillard, florent.gaillard@chuv.ch