Moving Picture, Audio and Data Coding
by Artificial Intelligence
www.mpai.community

MPAI Technical Specification

AI for Health (MPAI-AIH) – Health Secure Platform (AIH-HSP)

V1.0

WARNING

Use of the technologies described in this Technical Specification may infringe patents, copyrights or intellectual property rights of MPAI Members or non-members.

MPAI and its Members accept no responsibility whatsoever for damages or liability, direct or consequential, which may result from the use of this Technical Specification.

Readers are invited to review Notices and Disclaimers.

Technical Specification:
AI for Health (MPAI-AIH) – Health Secure Platform (AIH-HSP) V1.0

Contents

1 Foreword

The international, unaffiliated, non-profit ***Moving Picture, Audio, and Data Coding by Artificial Intelligence (MPAI)*** organisation was established in September 2020 in the context of:

1. **Increasing** use of Artificial Intelligence (AI) technologies applied to a broad range of domains affecting millions of people
2. **Marginal** reliance on standards in the development of those AI applications
3. **Unprecedented** impact exerted by standards on the digital media industry affecting billions of people

believing that AI-based data coding standards will have a similar positive impact on the Information and Communication Technology industry.

The design principles of the MPAI organisation as established by the MPAI Statutes are the development of AI-based Data Coding standards in pursuit of the following policies:

1. Publish upfront clear Intellectual Property Rights licensing frameworks.
2. Adhere to a rigorous standard development process.
3. Be friendly to the AI context but, to the extent possible, remain agnostic to the technology thus allowing developers freedom in the selection of the more appropriate – AI or Data Processing – technologies for their needs.
4. Be attractive to different industries, end users, and regulators.
5. Address five standardisation areas:
    1. *Data Type*, a particular type of Data, e.g., Audio, Visual, Object, Scenes, and Descriptors with as clear semantics as possible.
    2. *Qualifier*, specialised Metadata conveying information on Sub-Types, Formats, and Attributes of a Data Type.
    3. *AI Module* (AIM), processing elements with identified functions and input/output Data Types.
    4. *AI Workflow* (AIW), MPAI-specified configurations of AIMs with identified functions and input/output Data Types.
    5. *AI Framework* (AIF), an environment enabling dynamic configuration, initialisation, execution, and control of AIWs.
6. Provide appropriate Governance of the ecosystem created by MPAI Technical Specifications enabling users to:
    1. *Operate* Reference Software Implementations of MPAI Technical Specifications provided together with Reference Software Specifications
    2. *Test* the conformance of an implementation with a Technical Specification using the Conformance Testing Specification.
    3. *Assess* the performance of an implementation of a Technical Specification using the Performance Assessment Specification.

4. *Obtain* conforming implementations possibly with a performance assessment report from a trusted source through the MPAI Store.

MPAI operates on four solid pillars:

1. The MPAI Patent Policy specifies the MPAI standard development process and the Framework Licence development guidelines.
2. *Technical Specification: Artificial Intelligence Framework (MPAI-AIF)* V2.1 specifies an environment enabling initialisation, dynamic configuration, and control of AI applications in the standard AI Framework environment depicted in Figure 1. An AI Framework can execute AI applications called AI Workflows (AIW) typically including interconnected AI Modules (AIM). MPAI-AIF supports small- and large-scale high-performance components and promotes solutions with improved explainability.

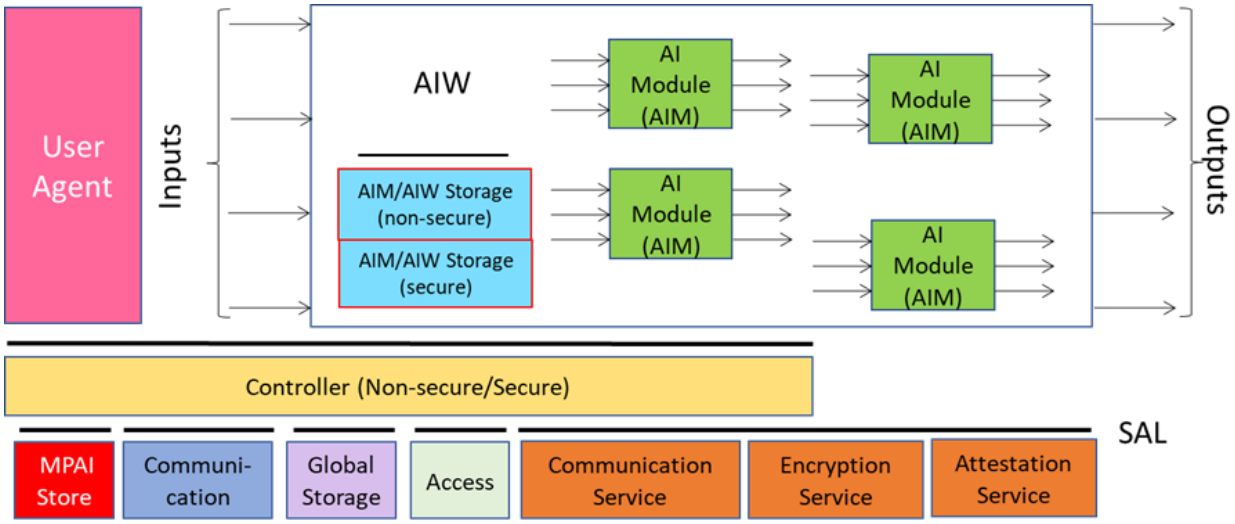

Figure 1 – The AI Framework (MPAI-AIF) V2 Reference Model

3. ***Technical Specification: Data Types, Formats, and Attributes (MPAI-TFA) V1.4*** specifies Qualifiers, a type of metadata supporting the operation of AIMs receiving data from other AIMs or from input data. Qualifiers convey information on Sub-Types (e.g., the type of colour), Formats (e.g., the type of compression and transport), and Attributes (e.g., semantic information in the Content). Although Qualifiers are human-readable, they are only intended to be used by AIMs. Therefore, Text, Speech, Audio, Visual, and other Data received by or exchanged between AIWs and AIMs should be interpreted as being composed of Content (Text, Speech, Audio, and Visual as appropriate) and associated Qualifiers. For instance, a Text Object is composed of Text Data and Text Qualifier. The specification of most MPAI Data Types reflects this point.
4. ***Technical Specification: Governance of the MPAI Ecosystem (MPAI-GME) V2.0*** defines the following elements:
    1. Standards, i.e., the ensemble of Technical Specifications, Reference Software, Conformance Testing, and Performance Assessment.
    2. Developers of MPAI-specified AIMs and Integrators of MPAI-specified AIWS (Implementers).
    3. MPAI Store in charge of making AIMs and AIWs submitted by Implementers available to Integrators and End Users.
    4. Performance Assessors, independent entities assessing the performance of implementations in terms of Reliability, Replicability, Robustness, and Fairness.
    5. End Users.

The interaction between and among actors of the MPAI Ecosystem are depicted in Figure 2.

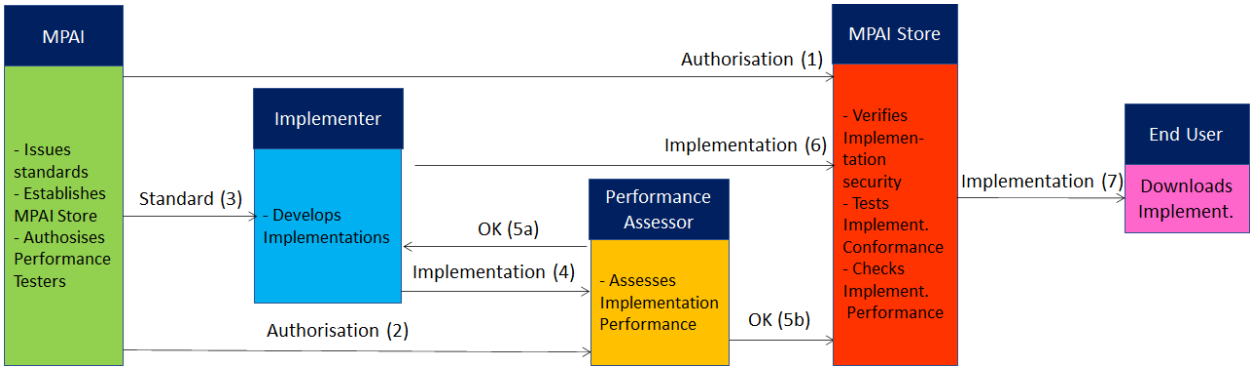

Figure 2 – The MPAI Ecosystem

2 Introduction (Informative)

Technical Specification: Artificial Intelligence for Health (MPAI-AIH) - Health Secure Platform (AIH-HSP) V1.0 – in the following also called AIH-HSP V1.0 or AIH-HSP – supports advanced forms of health services that enable End Users to acquire health data, convert it to a form that includes a licence through which the End User retains full control of who, how, and when another User processes their health data for what purpose.

The End User is required to equip themselves with a Health Front End that allows them to:

1. Register with the Health Secure Platform .
2. Acquire different types of Health Data.
3. Download AI Modules (AIM) from the MPAI Store.
4. Process their health data with AIMs while the AIMs learn.
5. Upload their health data to the back end of the Health Secure Platform
6. Grant Rights to the back end
    1. To perform certain processing on their health data, and
    2. To sublicense their AIH Data to qualified Third-Party Users.
7. Share their trained Neural Network Models with the Health Secure Platform's Back End.

The back end then produces and uploads to the MPAI Store a new version of that type of Neural Network Model with Federated Learning Technologies, Front ends can then for front ends can then download and use it.

Chapters and Sections are Normative unless they are explicitly identified as Informative.

Capitalised Terms are defined in *Table 1* if specific of this AIF-HSP V1.0 Technical Specification. All MPAI-defined Terms are accessible online.

Note: The development of MPAI-AIH V1.0 was stimulated by the "AI Health" Portuguese research project.

3 Scope

Technical Specification: Artificial Intelligence for Health (MPAI-AIH) - Health Secure Platform (AIH-HSP) V1.0 specifies:

1. The architecture of an end-to-end system called Secure Health Platform composed of:
    1. Front Ends that:
        1. Acquire Health Data.
        2. Process Health Data with AI Modules based on Neural Networks producing AI Health Data (AIH Data).
        3. License AIH Data to the Back End by attaching Model Licences to Health Data.

4. Share their Neural Network Models with the Health Back End for Federated Learning purposes.

2. A Back End that:
    1. Collects and stores AIH Data.
    2. Stores AIH Data Licences as Smart Contracts in a Blockchain.
    3. Processes AIH Data with AI Modules based on Neural Networks.
    4. Provides access to and enables Third-Party users to process AIH Data based on Smart Contracts.
    5. Collects Neural Network Models from Health Front Ends.
    6. Produces and distributes newer Neural Network Models by applying Federated Learning to the received Neural Network Models.
3. A Blockchain that manages Smart Contracts, representing Licence Models.

AIH-HSP specifies Taxonomies for Data, Processing, and Actors of the Health Secure Platform.
AIH-HSP relies on the following MPAI standards:

1. ***Technical Specification: Artificial Intelligence Framework (MPAI-AIF) V3.0*** specifying the AI Framework (AIF) where Health Data is processed by AI Modules (AIM).
2. ***Technical Specification: Process Instance Trust Framework (MPAI-PTF) V1.0*** specifying the data structures, processes, and protocols enabling AIMs to establish, evaluate, and maintain trust in the AIF**.**
3. ***Technical Specification: Data Types, Formats, and Qualifiers (MPAI-TFA) V1.4*** specifying the Health Data Type Qualifiers enabling AIH-HSP to specify Data Types the are independent of specific formats.

An AIH-HSP implementation should provide the functionalities of the Technical Specification in compliance with the relevant applicable legal frameworks such as the European Union General Data Protection Regulation (GDPR) [6] or Artificial Intelligence Act [7].
Technical Specification: Artificial Intelligence for Health (MPAI-AIH) - Health Secure Platform (AIH-HSP) V1.0 has been developed by the AI Health Development Committee (AIH-DC) of Moving Picture, Audio, and Data Coding by Artificial Intelligence (MPAI), the international, unaffiliated, non-profit organisation developing standards for AI-based data coding.
MPAI may develop new Versions or new Technical Specifications whose scope is related to the AIH-HSP V1.0 Technical Specification.

4 Definitions

Capitalised Terms used in this Technical Specification have the meaning defined in Table 1. Lower-case Terms have the meaning commonly defined for the context in which they are used. For instance, Table 1 defines *Licence* but does not define *licence*.
A dash "-" preceding a Term in Table 1 indicates the following readings according to the font:

1. Normal font: the Term in the table without a dash and preceding the one with a dash should be read before that Term. For example, "AIH Model" and "- Instance" will yield "AIH Model Instance".
2. *Italic* font: the Term in the table without a dash and preceding the one with a dash should be read after that Term. For example, "AI Health (AIH) Data" and "- *Processed*" will yield "Processed AI Health (AIH) Data".

Other Capitalised terms have been defined by other MPAI Technical Specifications. All MPAI-defined Terms are accessible online.

Table 1 – General MPAI-AIF terms

Term	Definition
Access	The process of a User or a Service to perform a data operation or function on the Health Secure Platform.
AI Framework (AIF)	The environment where AIWs are executed.
AI Health (AIH) Data	Health-related data entering the Health Secure Platform.
- Anonymisation	A mechanism that protects private or sensitive data by erasing or encrypting identifiers that connect an individual to stored data.
- De-identification	A mechanism that breaks the link between data and the individual with whom the data is initially associated. It is a type of data anonymization.
- *Processed*	AIH Data that have undergone processing by an AIH Data Processing AIM designed to perform transformative procedures such as extract features, assess disease evolution, etc.
AI Module (AIM)	A processing element receiving AIM-specific Inputs and producing AIM-specific Outputs according to according to its Function. An AIM may be an aggregation of AIMs.
AIH Model	An AIM trained model for processing AIH Data.
- Instance	A local End User instance of the AIH model.
AI Workflow (AIW)	A structured aggregation of AIMs implementing a Use Case receiving AIW-specific inputs and producing AIW-specific inputs according to its Function.
Health Secure Platform	The ICT platform offering AIH services.
- Back End	The part of the Health Secure Platform collecting, storing, and processing health data, and carrying out Federated Learning functions on the AI Models from the Front-end.
- Front-End	The end-user devices collecting and processing personal health data and updating the AI Models received from the Health Secure Platform Back End.
AIH Processing Taxonomy	The recognised set of processing that the Health Secure Platform Back End can execute.
Anonymisation	The process of removing or transforming personally identifiable information (PII) from data to make it impossible to identify an individual, even with additional information.
Audit	Process that determines if the services are safeguarding licencing and maintaining data integrity and privacy.
Authentication	Process of verifying and attesting the identification of a User or a Service.

Blockchain	A shared immutable ledger stored on a peer-to-peer network of computers.
External Communication	Set of services to communicate to a platform other than the Health Secure Platform.
External Source	A platform other than the Health Secure Platform from which the Health Secure Platform Back End may collect subsidiary data for the integration of relevant information for health-related predictions.
Federated Learning System (FLS)	The AIW system aggregating the data describing each of the Health Secure Model Instances for the update of a global Model for AIH system-wide distribution.
Licence	Document that creates a bond between a User, their AIH Data, the Health Secure Platform Back Ends, and any Third-Party User expressed by the conditions that regulate the access to that data.
Personally Identifiable Information	(PII) Any data that can be used to distinguish or trace an individual's identity, either alone or when combined with other information.
Provenance	A record trail that accounts for the origin of a piece of data (in a database, document, or repository) together with an explanation of how and why it got to the present place
Pseudonymisation	The processing of personal data in such a way that the data can no longer be attributed to a specific individual without the use of additional information, provided that this additional information is kept separately and is subject to technical and organisational measures to ensure non-attribution.
Secure Data Vault	A repository that holds several types of data in an encrypted format. Access to the data is controlled by the user through the presentation of appropriate credentials.
Service	Software functionality, or a set of software functionalities, such as the retrieval of specified information or the execution of a set of operations.
Smart Contract	A Program stored on a Blockchain that runs when activated by an external entity, e.g., a User or another Smart Contract.
Time series Data	**A** collection of data points collected over time (e.g., heartbeats /minute, brain electrical activity, electrocardiogram, etc.).
Token	A Data Type, e.g., name, password, biometrics, etc.
User	Any entity involved in or accessing the Health Secure Platform.
- *End*	The holder of an Health Secure Platform Front-End instance.
- *Third-Party*	An Entity – excluding the AIH System and the End User – accessing the Health Secure Platform Back End to process some stored AIH data.

5 References

5.1 Normative References

1. MPAI; Technical Specification; MPAI Ecosystem Governance (MPAI-GME) V2.0.
2. MPAI; Technical Specification; AI Framework (MPAI-AIF) V3.0.
3. MPAI; Technical Specification; AProcess Instance Trust Framework (MPAI-AIF) V3.0.
4. MPAI; Technical Specification; Data Types, Formats, and Attributes (MPAI-TFA) V1.4.

5.2 Informative References

5. MPAI; The MPAI Statutes.
6. MPAI; The MPAI Patent Policy.
7. MPAI; Framework Licence: AI for Health (MPAI-AIH).
8. General Data Protection Regulation (GDPR) https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en (Accessed 20th July 2023).
9. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

6 Architecture

The Health Secure Platform (HSP) is a system composed of a Health Back End (HBE), a plurality of Health Front Ends (HFE), and a Blockchain. End Users and Third-Party Users access the Health Secure Functions as describes in the Operation Section.
Figure 1 graphically depicts the elements of the AI for Health - Secure Platform.

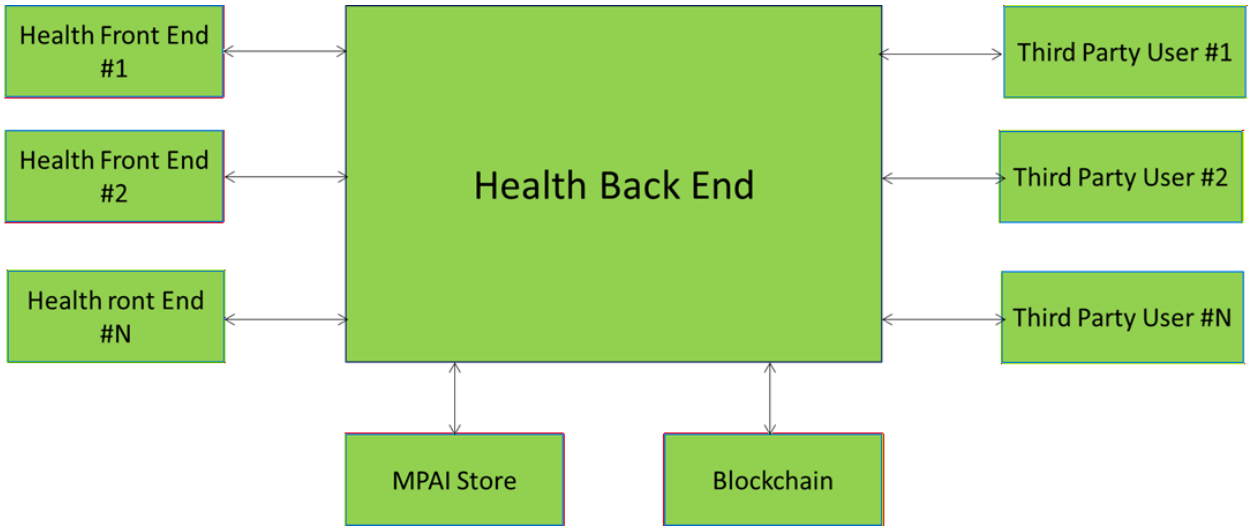

Figure 1 - General Model of AIH-HSP V1.0

6.1 Operation

The operation of the HSP is best described by this workflow:

1. An End User
    1. Is equipped with device running an AIF-enabled app - Health Front End (HFE).
    2. Acquires and uniquely identify Health Data.

3. Creates AIH Data by combining Health Data with a Model Licence and uniquely identifying it.
4. Processes AIH Data using AI Modules (AIM) downloaded from the MPAI Store. Neural Networks in the AIMs continually learn while making inferences on AIH Data.
5. Creates a new uniquely identified AIH Data instance.
6. Uploads un-processed and processed AIH Data to the Health Back End

2. The Health Back End
    1. Downloads the latest AIMs from the MPAI Store.
    2. Stores the Model Licence as a Smart Contract on a Blockchain.
    3. Converts the Model Licence into a Smart Contract.
    4. Add the ID of the Smart Contract to the AIH Data.
    5. Processes the AIH Data in the internal AI Framework as permitted by the terms and conditions expressed in the Smart Contract.
    6. From time to time sends a request to a class of End Users to receive the trained Neural Network Model with a specific untrained Model ID
3. Requested End Users send their trained Neural Network Models.
4. Health Back End
    1. Produces a new Neural Network Model from the received trained Models using Federated Learning techniques.
    2. Uploads the new Neural Network Model to the MPAI Store.
    3. Notifies End Users that the new Neural Network Model is available at the MPAI Store.
5. A Third-Party User belonging to one of the categories identified in the AI Health Taxonomy
    1. Registers with the Health Back End.
    2. Processes the AIH Data in the internal AI Framework as permitted by the terms and conditions expressed in the Smart Contract.
    3. Uses the processes AIH Data as permitted by the terms and conditions expressed in the Smart Contract.

The AIH Taxonomy identifies:

1. Users: currently: End User, Non-Profit Entity, Profit Entity, Clinical Entity, Authorised Entity, Caregiver.
2. AIH Data
    1. Classes (currently: ECG, EEG, Genomics, and Medical Images).
    2. Statuses (currently, Anonymised, Pseudonymised, Identified)
    3. Usages (currently, Unrestricted, Pseudonymised, Anonymised, Research, Patient use, Health care)
    4. Processing Types (currently: ECG, EEG, Genomics, and Medical Images).
3. Algorithms:
    1. Anonymisation
    2. De-Identification
4. Anomalies: Types.

Note that the Operation of an implementation of an AIF instance is required to be Zero Trust. Technical Specification: AI Framework (MPAI-AIF) V3.0 provides a set of requirements that a Zero-Trust implementation of an AIF instance is expected to satisfy.

6.2 Services

The Health Secure Platform is composed of a set of distributed components and services:

1. The *Front End*, the End User's personal gateway to their external biometric sensors and any AIH Data that:
    1. Captures End User's Health Data, e.g., from Google Fit and Apple Health, and external biometric sensors that capture Health Data.
    2. Locally stores AIH Data in a "Secure Data Vault" controlled by the End User.
    3. AI processes AIH Data using standard AIMs and AIWs downloaded from the MPAI-Store performing the computational operations on the End User's AIH Data, including transformations, training, and inferences.
    4. Alerts the End-User about any deviation of the value of the AIH Data that may be caused, e.g., by disease, injury, or chronic conditions.
    5. Uploads the processed AIH Data to the Back End.
2. The *AIH Back End*, composed of a set of tools that implement the necessary services
    1. Securely stores, de-identifies and anonymises AIH Data, controls entity authentication and access to data, and licenses and audits the access to Back End AIH Data.
    2. Gathers anonymised data from End Users and acts as a broker gateway between Third-Part Entities requesting access to AIH Data and its providers.
    3. Grants access rights without referring to the identity of the End Users providing the data. The Back End may only grant the Third-Party User the rights to process AIH Data that the Back End has been specifically granted by the relevant End User.
3. *Blockchain* enables the system's transparency and auditability. Each provision of and access to AIH Data requires the emission of a license in the form of a Smart Contract that is stored on the Blockchain. The Smart Contract contains information about:
    1. The parties, e.g., the End User sending AIH Data and the Back End, and any future Third-Party User requesting access to and processing AIH Data.
    2. The Type of Third-Party User (per the MPAI-AIH Taxonomy).
    3. The AIH Data and AIH Models to be used.
    4. The Rights granted to use the AIH Data:
        1. Type of use of the AIH Data (per the MPAI-AIH Taxonomy).
        2. Type of use of the processed AIH Data (per the MPAI-AIH Taxonomy).
    5. The duration of the Licence.
4. The *AI Services* offered by the Back End can be used directly to process the AIH Data on the Front End and extract the specific knowledge sought by the End User or Third-Party Users based on the Licence. These services are selected from those available from the MPAI Store and may be orchestrated to produce specific analyses for the Third-Party Users that request access to AIH Data. By means of data processing, AI services enable specific and customised training of Machine Learning Models to identify and assist in the identification of medical diagnosis and prognosis.
5. The AI *Federated Learning System* (FLS) orchestrates the learning of a central model for medical diagnosis and prognosis, namely by working as a medical anomaly detection tool, receiving Neural Network Model weights data from the Front End and using it under the terms of the Smart Contract that was established between the End User and the Back End. When an improved model is obtained by the FLS, this is uploaded to the MPAI-Store.

6.3 Security

The Front Ends and the Back End are implemented as AI Frameworks specified by the Technical Specification: AI Framework (MPAI-AIF). After trust has been established between a Front End and the Back End or between the AIMs in a Front End or in the Back End as specified by Technical Specification: Process Instance Trust Framework (MPAI-PTF), interactions and data exchange becomes possible and Data Exchange Metadata can be added to any data instance.

7 AI Modules

7.1 Technical Specifications

Table 1 provides the links to the specifications and the JSON schemas of all AIMs specified by ***Technical Specification: AI for Health (MPAI-AIH) - Health Secure Platform (AIH-HSP) V1.0***.

Table 1 - Specifications and JSON syntax of AIMs used by MPAI-AIH V1.0

Acronym	Name	JSON	Acronym	Name	JSON
AIH-HDP	AIH Data Processing	X	AIH-HBE	Health Back End	X
AIH-ARA	Anomaly and Risk Alerting	X	AIH-HFE	Health Front End	X
AIH-ADT	Auditing	X	AIH-MDL	Model Licensing	X
AIH-DIA	De-Identification and Anonymisation	X	AIH-STR	Storage	X
AIH-HFL	Health Federated Learning	X			

7.1.1 AIH Data Processing

7.1.1.1 Functions

The AIH Data Processing (AIH-HDP) AIM performs one of processing functions on AIH Data:

Receives	Licence Confirm Response	Response to request to confirm Licence ID.
	Blockchain Licence Response	Response to Blockchain Licence Request.
	Federated Learn Response	Response to Federated Learn Request.
	AIH Data Process Response	Health Back End's response to request to Process AIH Data.
	AIH Data	AIH Data.
	AIH Data Process Request	Request to Health Back End to Process AIH Data.
	ARA Data	Anomaly and Risk Alert Data
Produces	Licence Confirm Request	Request to Blockchain to confirm Licence ID.
	Blockchain Licence Request	Request to Blockchain to create Smart Contract.
	Federated Learn Request	Request to provide trained NN Model.
	AIH Data Store Request	Request from to Store AIH Data.
	AIH Data	Processed AIH Data.

7.1.1.2 Reference Model

The AIH Data Processing (AIH-HDP) AIM Reference Model is depicted in Figure 1.

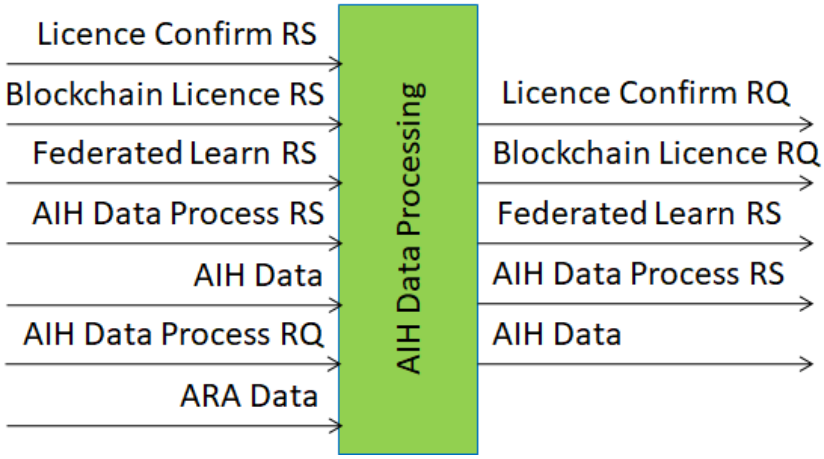

Figure 1 – AIH Data Processing (AIH-HDP) AIM Reference Model

7.1.1.3 Input/Output Data

Table 1 specifies the Input and Output Data of the AIH Data Processing (AIH-HDP) AIM. Links are to the Data Type specifications.

Table 1 – I/O Data of the AIH Data Processing (AIH-HDP) AIM

Input	Description
Licence Confirm Response	Response to request to confirm Licence ID.
Blockchain License Response	Response to Blockchain Licence Request.
Federated Learn Response	Response to Federated Learn Request. This data is provided only by an AIH Data Processing Instance of the Health Back End.
AIH Data Process Response	Health Back End's response to request to Process AIH Data.
AIH Data	AIH Data.
AIH Data Process Request	Request to Health Back End to Process AIH Data.
ARA Data	Anomaly and Risk Alert Data
Output	**Description**
Licence Confirm Request	Request to Blockchain to confirm Licence ID.
Blockchain License Request	Request to Blockchain to create Smart Contract.
Federated Learn Response	Response to request to provide trained NN Model. This data is provided only by an AIH Data Processing Instance of the Health Back End.
AIH Data Process Response	Response to the Request to process AIH data.

AIH Data	Processed AIH Data.

7.1.1.4 JSON Metadata

https://schemas.mpai.community/AIH1/V1.0/AIMs/AIHDataProcessing.json

7.1.1.5 Conformance Testing

Table 2 provides the Conformance Testing Method for AIH Data Processing (AIH-HDP) AIM.

If a schema contains references to other schemas, conformance of data for the primary schema implies that any data referencing a secondary schema shall also validate against the relevant schema, if present and conform with the Qualifier, if present.

Table 2 – Conformance Testing Method for AIH Data Processing (AIH-HDP) AIM

Receives	Licence Confirm Response	Shall validate against Licence Confirm schema.
	Blockchain Licence Response	Shall validate against Blockchain Licence schema.
	Federated Learn Response	Shall validate against Federated Learn schema.
	AIH Data Process Response	Shall validate against AIH Data Process schema.
	AIH Data	Shall validate against AIH Data schema.
	AIH Data Process Request	Shall validate against AIH Data Process schema.
	ARA Data	Shall validate against ARA Data schema.
Produces	Licence Confirm Request	Shall validate against Licence Confirm schema.
	Blockchain Licence Request	Shall validate against Blockchain Licence schema.
	Federated Learn Request	Shall validate against Federated Learn schema.
	AIH Data Process Request	Shall validate against AIH Data Process schema.
	AIH Data	Shall validate against AIH Data schema.

7.1.2 Anomaly and Risk Alerting

7.1.2.1 Functions

The Anomaly and Risk Alerting (AIH-ARA) AIM checks data AIH Data do not signal anomalies:

Receives AIH Data
Produces ARA Data

7.1.2.2 Reference Model

The Anomaly and Risk Alerting (AIH-ARA) AIM Reference Model is depicted in Figure 1.

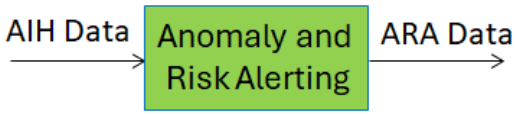

Figure 1 – The Anomaly and Risk Alerting (AIH-ARA) AIM Reference Model

7.1.2.3 Input/Output Data

Table 1 specifies the Input and Output Data of the Anomaly and Risk Alerting (AIH-ARA) AIM. Links are to the Data Type specifications.

Table 1 – I/O Data of the Anomaly and Risk Alerting (AIH-ARA) AIM

Input	Description
AIH Data	Data leaving the HFE Processing AIM because it is suspected to have an anomaly..
Output	**Description**
ARA Data	Data indicating the anomaly detected by the AIH-ARA AIM.

7.1.2.4 JSON Metadata

https://schemas.mpai.community/AIH1/V1.0/AIMs/AnomalyAndRiskAlerting.json

7.1.2.5 Conformance Testing

Table 2 provides the Conformance Testing Method for Anomaly and Risk Alerting (AIH-ARA) AIM.

If a schema contains references to other schemas, conformance of data for the primary schema implies that any data referencing a secondary schema shall also validate against the relevant schema, if present and conform with the Qualifier, if present.

Table 2 – Conformance Testing Method for Anomaly and Risk Alerting (AIH-ARA) AIM

Receives	AIH Data	Shall validate against AIH Data schema.
Produces	ARA Data	Shall validate against ARA Data schema.

7.1.3 Auditing

7.1.3.1 Functions

The Auditing (AIH-ADT) AIM checks whether unlicensed processing has been performed on AIH Data:

Receives	Audit Request	Request to Audit Data.
	AIH Data	AIH Data to be Audited identified by its ID.
	Licence Confirm Response	Response to Request to Blockchain to confirm Licence ID.
Produces	Audit Response	Response of to Request to Audit Data.
	Licence Confirm Request	Request to Blockchain to confirm Licence ID.

7.1.3.2 Reference Model

The Auditing (AIH-ADT) AIM Reference Model is depicted in Figure 1.

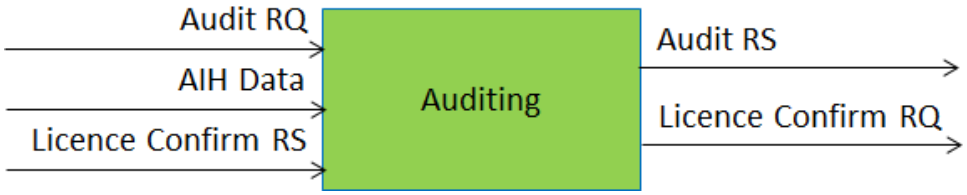

Figure 1 – The Auditing (AIH-ADT) AIM Reference Model

7.1.3.3 Input/Output Data

Table 1 specifies the Input and Output Data of the Auditing (AIH-ADT) AIM. Links are to the Data Type specifications.

Table 1 – I/O Data of the Auditing (AIH-ADT) AIM

Input	Description
Audit Request	Request to Audit Data.
AIH Data	AIH Data to be Audited.
Licence Confirm Response	Response to Request to Blockchain to confirm Licence ID.
Output	**Description**
Audit Response	Response of Audit containing a list of non-conformities: - Processing Type - Requesting User - Date of Request - Processing status (executed/denied).
Licence Confirm Request	Request to Blockchain to confirm Licence ID.

7.1.3.4 JSON Metadata

https://schemas.mpai.community/AIH1/V1.0/AIMs/Auditing.json

7.1.3.5 Conformance Testing

Table 2 provides the Conformance Testing Method for Auditing (AIH-ADT) AIM.

If a schema contains references to other schemas, conformance of data for the primary schema implies that any data referencing a secondary schema shall also validate against the relevant schema, if present and conform with the Qualifier, if present.

Table 2 – Conformance Testing Method for Auditing (AIH-ADT) AIM

Receives	Audit Request	Shall validate against Audit schema.
	AIH Data	Shall validate against AIH Data schema.
	Licence Confirm Response	Shall validate against Licence Confirm schema.
Produces	Audit Response	Shall validate against Audit schema.
	Licence Confirm Request	Shall validate against Licence Confirm schema.

7.1.4 De-Identification and Anonymisation

7.1.4.1 Functions

The De-Identification and Anonymisation (AIH-DIA) AIM de-identifies or anonymises AIH Data:

Receives	De-ID and Anonym Request	Request to De-Identify and Pseudo-Anonymise Data.
	AIH Data	Data to be De-Identified and Pseudo-Anonymised.
Produces	De-ID and Anonym Response	Response to request to De-Identify and Pseudo-Anonymise Data.
	AIH Data	Data De-Identified and Pseudo-Anonymised.

7.1.4.2 Reference Model

The De-Identification and Anonymisation (AIH-DIA) AIM Reference Model is depicted in Figure 1.

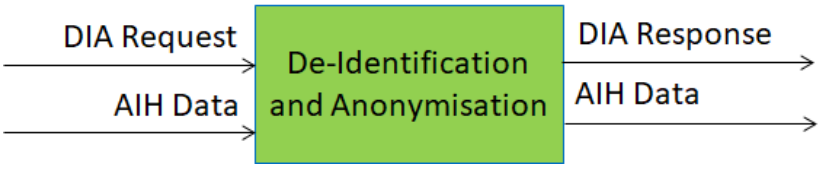

Figure 1 – The De-Identification and Anonymisation (AIH-DIA) AIM Reference Model

7.1.4.3 Input/Output Data

Table 1 specifies the Input and Output Data of the De-Identification and Anonymisation (AIH-DIA) AIM. Links are to the Data Type specifications.

Table 1 – I/O Data of the De-Identification and Anonymisation (AIH-DIA) AIM

Input	Description
De-ID and Anonym Request	Request to De-Identify or Anonymise Data.
AIH Data	Data to be De-Identified or Anonymised.
Output	**Description**
De-ID and Anonym Response	Response to request to De-Identify or Anonymise Data.
AIH Data	Data De-Identified or Anonymised.

7.1.4.4 JSON Metadata

https://schemas.mpai.community/AIH1/V1.0/AIMs/DeIdentificationAndAnonymisation.json

7.1.4.5 Conformance Testing

Table 2 provides the Conformance Testing Method for De-Identification and Anonymisation (AIH-DIA) AIM.

If a schema contains references to other schemas, conformance of data for the primary schema implies that any data referencing a secondary schema shall also validate against the relevant schema, if present and conform with the Qualifier, if present.

Table 2 – Conformance Testing Method for De-Identification and Anonymisation (AIH-DIA) AIM

Receives	De-ID and Anonym Request	Shall validate against De-ID and Anonym schema.
	AIH Data	Shall validate against AIH Data schema.
Produces	De-ID and Anonym Response	Shall validate against De-ID and Anonym schema.
	AIH Data	Shall validate against De-ID and Anonym schema.

7.1.5 Health Federated Learning

7.1.5.1 Functions

The Health Federated Learning (AIH-HFL) AIM Integrates into a new NN Model the knowledge acquired by trained NN Module participating in the Federated Learning Process:

Receives	Federated Learning Response	Response to Federated Learning Request (NN Model)
Produces	Neural Network Model	NN Model submitted to MPAI Store
	Federated Learning Request	Request to Health Front End for a given NN Model

7.1.5.2 Reference Model

The Health Federated Learning (AIH-HFL) AIM Reference Model is depicted in Figure 1.

Figure 1 – The Health Federated Learning (AIH-HFL) AIM Reference Model

7.1.5.3 Input/Output Data

Table 1 specifies the Input and Output Data of the The Health Federated Learning (AIH-HFL) AIM. Links are to the Data Type specifications.

Table 1 – I/O Data of theThe Health Federated Learning (AIH-HFL) AIM

Input	Description
Federated Learn Response	Response to Federated Learning Request (NN Model).
Output	**Description**
NN Model	NN Model submitted to MPAI Store.
Federated Learn Request	Request to Health Front End for a given NN Model.

7.1.5.4 JSON Metadata

https://schemas.mpai.community/AIH1/V1.0/AIMs/HealthFederatedLearning.json

7.1.5.5 Conformance Testing

Table 2 provides the Conformance Testing Method for Health Federated Learning (AIH-HFL) AIM.

If a schema contains references to other schemas, conformance of data for the primary schema implies that any data referencing a secondary schema shall also validate against the relevant schema, if present and conform with the Qualifier, if present.

Table 2 – Conformance Testing Method for OSD-EVD AIM

Receives	Federated Learn Response	Shall validate against Federated Learning schema.
Produces	NN Model	Shall validate against ML Model schema.
	Federated Learn Request	Shall validate against Federated Learning schema.

7.1.6 Health Back End

7.1.6.1 Functions

The Health Back End (AIH-HBE) AIM implements the following functionalities:

Receives	Federated Learn Response	Health Front End's response to request to provide its trained NN.
	Audit Request	Health Front End's to Audit AIH Data.

	Licence Confirm Response	Blockchain's response to Licence Confirmation Request.
	DIA Requests	Request to De-Identify and Anonymise AIH Data.
	Blockchain Licence Response	Blockchain's Response to Request to create Smart Contract from Model Licence.
	Licence Confirm Response	Response to Request to Blockchain to confirm Licence ID.
	AIH Data Process Request	Request to Process AIH Data.
	Register Request	User's Request to Register.
Produces	NN Model	Neural Network sent by Health Front End.
	Federated Learn Request	Request to Health Front End to provide its trained NNs.
	Audit Response	Response to request to Audit AIH Data.
	Licence Confirm Request	Request to Blockchain to confirm Licence ID.
	DIA Response	Health Back End's response to request to De-Identify and Anonymise AIH Data.
	Blockchain Licence Request	Blockchain's request to create Smart Contract from Model Licence.
	AIH Data Process Response	Health Back End's response to request to Process AIH Data.
	Register Response	Health Back End's response to User's Request to Register.

7.1.6.2 Reference Model

Figure 1 depicts the Reference Model of the Health Back End (AIH-HBE) AIM.

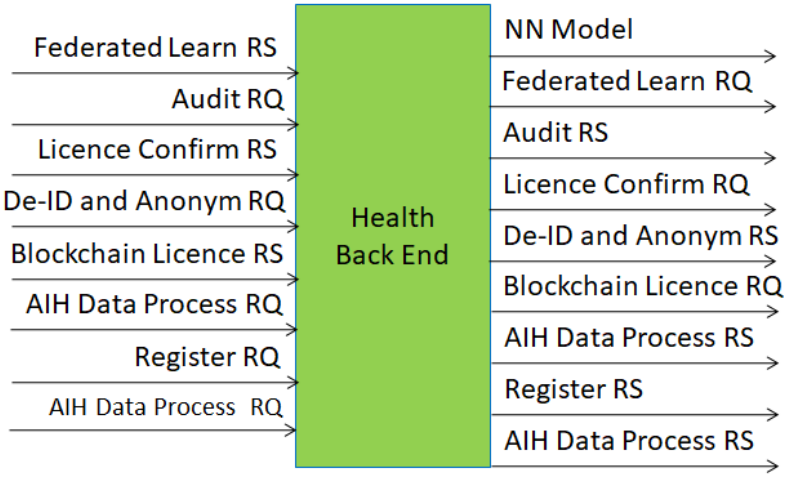

Figure 1 – Reference Model of the Health Back End (AIH-HBE) AIM

7.1.6.3 I/O Data

Table 1 specifies the Input and Output Data.

Table 1 – I/O Data of Health Back End (AIH-HBE) AIM

Input	Description
Federated Learn Request	HBE's request to End User to produce NN Model.
Audit Request	User's request to Audit Processing of AIH Data.
Licence Confirm Response	Blockchain response to request to confirm that a specific Processing on specific AIH Data is allowed by Licence.
De-ID and Anonym Request	User's request to De-Identify and Anonymise AIH Data.
Blockchain Licence Response	Blockchain's response to request to provide ID of Licence based on Model Licence
Licence Confirm Response	Blockchain response to a request that a specific Processing on specific AIH Data is allowed by Licence
AIH Data Process Request	User's request to Process AIH Data.
Register Request	User's request to Register
Output	**Description**
ML Model Object	NN Model sent to MPAI Store after completing Federated Learning process.
Federated Learn Response	Health Front End's response to Federated Learning Request.
Audit Request	User's request to Audit AIH Data for Processing.
Licence Confirm Request	Request to Blockchain that a specific Processing on specific AIH Data is allowed by Licence
De-ID and Anonym Response	HBE Data Processing's response to DIA Request.
Blockchain Licence Request	Request to Blockchain for Licence.
Licence Confirm Request	Blockchain response to a request that a specific Processing on specific AIH Data is allowed by Licence
AIH Data Process Response	HBE Data Processing's response to User's AIH Data Processing Request.
Register Response	Register Response to End User.

7.1.6.4 SubAIMs

7.1.6.4.1 Reference Model

Figure 2 depicts the Reference Architecture of the Health Back End (AIH-HBE) where Back End, End Users, Blockchain, and Third-Party Users perform operation. The term User indicates both End User and Third-Party User.

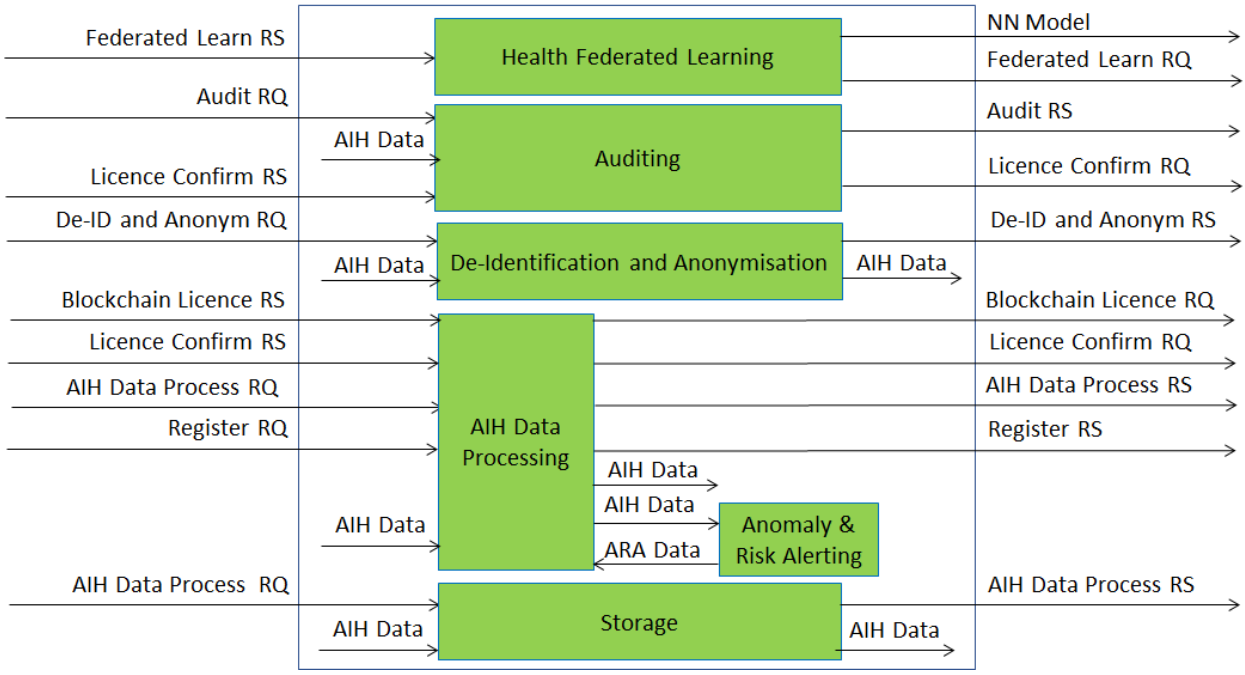

Figure 1 - Reference Model of the Health Back End (AIH-HBE) AIW

7.1.6.4.2 Operation

1. Back End accesses the MPAI Store and downloads the AIMs required for its operation.
2. User Registers
    1. A User wishing to access the Back End, sends a Registration Request containing Personal Profile and list of Service they intend to access.
    2. Back End provides the Tokens enabling the requesting User to access the corresponding Services.
3. Storage of AIH Data
    1. End User uploads AIH Data.
    2. HBE Data Processing
        1. Extracts Model Licence from AIH Data.
        2. Issues Blockchain Licence Request to Blockchain.
    3. Blockchain
        1. Converts Model Licence to a Smart Contract.
        2. Responds with a Blockchain Licence Request.
    4. HBE Data Processing
        1. Attaches Blockchain Licence ID to AIH Data.
        2. Stores AIH Data in Secure Storage
4. De-Identification/Anonymisation (DIA) of AIH Data
    1. End User sends a DIA Request.
    2. HBE Data Processing
        1. Retrieves relevant AIH Data from Secure Storage.
        2. (Pseudo-)Anonymises AIH Data.
        3. Stores (Pseudo-)Anonymised AIH Data back to Secure Storage.
        4. Responds with a DIA Response.
5. AIH Data Processing

1. User sends AIH Process Request.
2. HBE Data Processing sends a Licence Confirm Request to the Blockchain.
3. Blockchain responds with a Licence Confirm Response.
4. HBE Data Processing
    1. Performs the requested Processing, if this is included in the Licence.
    2. Stores the Processed AIH Data as new AIH Data.
    3. Responds with an AI Data Process Response.

6. Audit
    1. End User sends Audit Request.
    2. Auditing
        1. Retrieves relevant Confirmation Responses.
        2. Responds with Audit Response.
7. Federated Learning
    1. Federated Learning sends Federated Learning Request to all Health Front Ends.
    2. Health Front Ends provide the NN Models.
    3. Federated Learning
        1. Develops and upload the new NN Model to the MPAI Store.
        2. Sends Federated Learning Response to Health Front Ends.
    4. Front Ends download the new NN Model from the MPAI Stor

7.1.6.4.3 Functions of AI Modules

Table 2 specifies the Function of the AI Modules.

Table 2 - Functions of Health Back End AI Modules

Sub-AI Module	Description
Health Federated Learning	Performs Federated Learning of Front Ends' NN Model.
Auditing	Enables End User to monitor the use of their AIH Data.
De-Identification and Anonymisation	De-identifies/(pseudo-)anonymise AIH Data.
AIH Data Processing	Processes AIH Data.
Anomaly and Risk Alerting	
Storage	Stores AIH Data (a type of AIH Processing)

7.1.6.4.4 I/O Data of AI Modules

Table 3 specifies the Input and Output Data of the AI Modules.

Table 3 - Input and Output Data of the AI Modules

AI Module	Receives	Produces
Health Federated Learning	Federated Learn Response	NN Model
		Federated Learn Request
Auditing	Audit Request	Audit Response
	Licence Confirm Response	Licence Confirm Request
De-Identification and Anonymisation	De-ID and Anonym Request	De-ID and Anonym Response
	AIH Data	AIH Data

AIH Data Processing	Blockchain License Response	Blockchain License Request
	Licence Confirm Response	Licence Confirm Request
	AIH Data Process Request	AIH Data Process Response
	Register Request	Register Response
	AIH Data	AIH Data
	ARA Data	
Storage	AIH Data Process Request	AIH Data Process Response
	AIH Data	AIH Data

7.1.6.4.5 AIMs and JSON Metadata

Table 4 provides the links to the AIM specifications and to the JSON syntaxes. AIM1 indicates the Composite AIM and AIM2 their SubAIMs.

Table 4 – AIMs and JSON Metadata

AIM1	AIM2	Name	JSON
AIH-HBE		Health Back End	X
	AIH-HFL	Health Federated Learning	X
	AIH-ADT	Auditing	X
	AIH-DIA	De-Identification and Anonymisation	X
	AIH-HDP	AIH Data Processing	X
	AIH-ARA	Anomaly and Risk Alerting	X
	AIH-STR	Storage	X

7.1.6.5 JSON Metadata

https://schemas.mpai.community/AIH1/V1.0/AIMs/HealthBacktEnd.json

7.1.7 Health Front End

7.1.7.1 Functions

The Health Front End (AIH-HFE) AIM enables the End User to

1. Register with the Health Back End.
2. Use Health Devices to collect various types of Health Data.
3. Provide a Model Licence to each Health Data collected.
4. Request the Health Front End to Process AIH Data.
5. Send AIH Data to the Health Back End.
6. Request The Back End to Process AIH Data.

The Health Front End

1. Stores AIH Data as combination of Model Licence and Health Data.
2. Processes AIH Data.
3. Adds Anomaly and Risk Alerting (ARA) Data, if present, to each AIH Data.
4. Receives requests for trained NN Models from Health Back End.
5. Sends its trained NN Models to the Health Back End for Federated Learning.

The End User owning the Front End is not bound by the Model Licence.

7.1.7.2 Reference Model

Figure 2 depicts the Reference Model of the Health Front End (AIH-HFE) AIM.

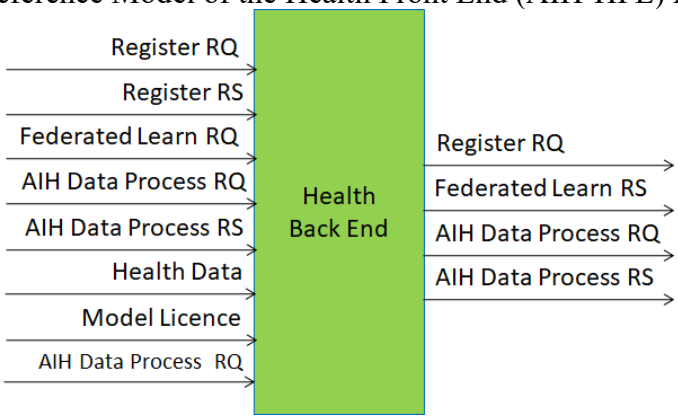

Figure 2 – Reference Model of the Health Front End (AIH-HFE) AIM

7.1.7.3 I/O Data

Table 1 specifies the Input and Output Data of the Health Front End (AIH-HFE) AIM.

Table 1 – I/O Data of Health Front End (AIH-HFE) AIM

Input	Description
Register Request	End User's request to Register.
Register Response	Data in response to a request to Register.
Federated Learn Request	Request to provide an NN Model.
AIH Data Process Request	End User's Request to process specific AIH Data
AIH Data Process Response	End User's Request to process specific AIH Data
Health Data	Data from End User's health device.
Model Licence	Data Describing End User's Licensing Terms and Conditions.
AIH Data	AIH Data to be stored.
Output	**Description**
Register Response	Register Response to End User.
AIH Data Process Request	End User's Request to process specific AIH Data.
AIH Data Process Response	Response to End User's Request to process specific AIH Data.
Federated Learn Response	Response to the request to provide an NN Model.
AIH Data	AIH Data retrieved.

7.1.7.4 SubAIMs

7.1.7.4.1 Reference Model

Figure 1 depicts the Reference Model of the Health Front End (AIH-HFE).

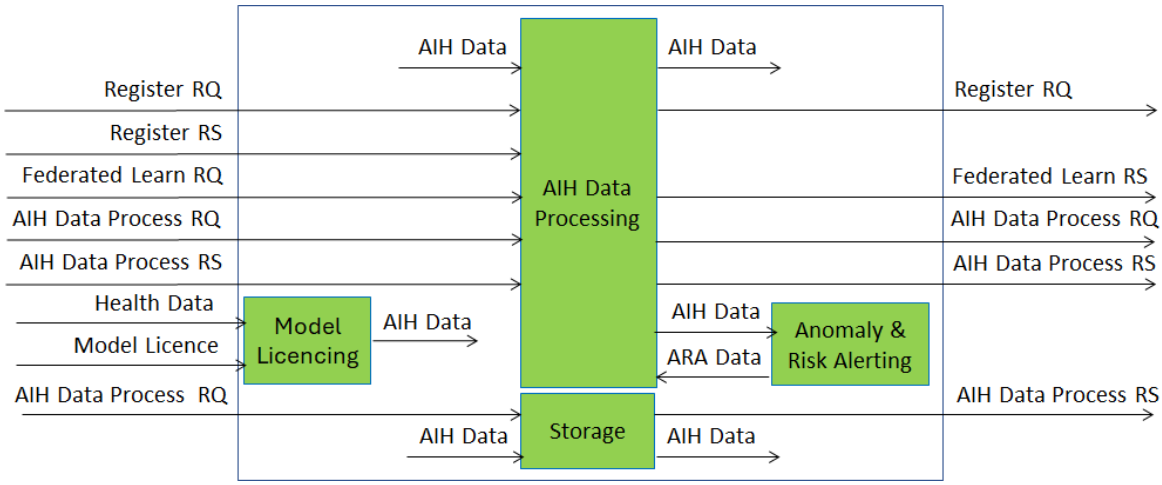

Figure 1 - Reference Model of the Health Front End (AIH-HFE) AIW

7.1.7.4.2 Operation

The AIH-HFE AIM operation develops as follows

1. End User registers with HFE and HBE.
2. End User acquire Health Data with a Health Device.
3. End User attaches Model Licence to Health Data.
4. Model Licencing stores AIH Data (including Health Data and Model Licence).
5. End User process AIH Data locally.
6. End User stores AIH Data to HFE.
7. End User process AIH Data remotely.
8. HFE receives Federated Learn request.
9. HFE sends NN Model to HBE.

7.1.7.4.3 Functions of AI Modules

Table 2 specifies the Function of the AIH-HFE AIM's SubAIMs.

Table 2 - Function of the AIH-HFE AIM's SubAIMs

AI Module	Description
Model Licensing	Adds Model Licence to Health Data.
AIH Data Processing	Processes AIH Data.
Anomaly and Risk Alerting	Discovers Anomalies and signals Risks in AIH Data.
Storage	Stores and retrieves AIH Data.

7.1.7.4.4 I/O Data of AI Modules

Table 3 specifies the Function of the AIH-HFE AIM's SubAIMs.

Table 3 - Functions of AIH-HFE AIM's SubAIMs

Acronym	AI Module	Receives	Produces
AIH-MDL	Model Licensing	Health Data	AIH Data
		Model Licence	
AIH-HDP	AIH Data Processing	Federated Learn Request	Federated Learn Response
		AIH Data Process Request	AIH Data Process Response

		AIH Data Process Response	AIH Data Process Request
		Health Data	
		Model Licence	
AIH-ARA	Anomaly and Risk Alerting	AIH Data	ARA Data
		Register Request	
		Register Response	
AIH-STR	Storage	AIH Data Process Request	AIH Data Process Response
		AIH Data	AIH Data

7.1.7.4.5 AIMs and JSON Metadata

Table 4 provides the links to the AIM specifications and to the JSON syntaxes. AIM1 indicates the Composite AIM and AIM2 their SubAIMs.

Table 4 – AIMs and JSON Metadata

AIM1	AIM2	Name	JSON
AIH-HFE		Health Front End	X
	AIH-MDL	Model Licensing	X
	AIH-HFP	AIH Data Processing	X
	AIH-ARA	Anomaly and Risk Alerting	X
	AIH-STR	Storage	X

7.1.7.4.6 JSON Metadata

https://schemas.mpai.community/AIH1/V1.0/AIMs/HealthFrontEnd.json

7.1.8 Model Licensing

7.1.8.1 Functions

The Model Licensing (AIH-MDL) AIM transforms Health Data into AIH Data by adding a Model Licence:

Receives	Health Data	Health Data of End User.
	Model Licence	Model Licence provided by End User for its Health Data.
Produces	AIH Data	Health Data with added Model Licence.

7.1.8.2 Reference Model

The Model Licensing (AIH-MDL) AIM Reference Model is depicted in Figure 1.

Figure 1 – The Model Licensing (AIH-MDL) AIM Reference Model

7.1.8.3 Input/Output Data

Table 1 specifies the Input and Output Data of the Anomaly and Risk Alerting (AIH-ARA) AIM. Links are to the Data Type specifications.

Table 1 – I/O Data of the Anomaly and Risk Alerting (AIH-ARA) AIM

Input	Description
Health Data	Health Data of End User.
Model Licence	Model Licence provided by End User for its Health Data.
Output	**Description**
AIH Data	Health Data with added Model Licence.

7.1.8.4 JSON Metadata

https://schemas.mpai.community/AIH1/V1.0/AIMs/ModelLicencing.json

7.1.8.5 Conformance Testing

Table 2 provides the Conformance Testing Method for Anomaly and Risk Alerting (AIH-ARA) AIM.

If a schema contains references to other schemas, conformance of data for the primary schema implies that any data referencing a secondary schema shall also validate against the relevant schema, if present and conform with the Qualifier, if present.

Table 2 – Conformance Testing Method for Anomaly and Risk Alerting (AIH-ARA) AIM

Receives	Health Data	Shall validate against AIH Data schema.
	Model Licence	Shall validate against Model Licence schema.
Produces	AIH Data	Shall validate against ARA Data schema.

7.1.9 Storage

7.1.9.1 Functions

The Storage (AIH-STR) AIM stores AIH Data:

Receives	AIH Data Process Request	Request to Process Data.
	AIH Data	AIH Data to be Processed.
Produces	AIH Data Process Response	Response of to Request to Process Data.

7.1.9.2 Reference Model

The Storage (AIH-STR) AIM Reference Model is depicted in Figure 1.

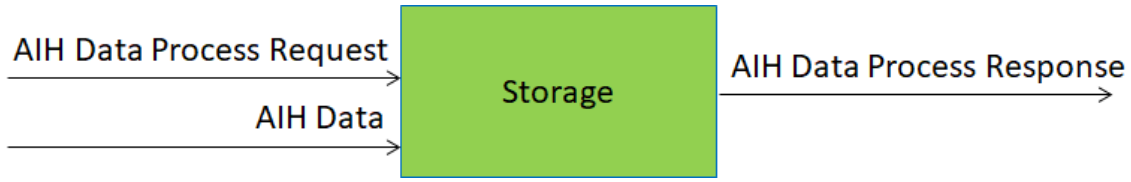

Figure 1 – The Storage (AIH-STR) AIM Reference Model

7.1.9.3 Input/Output Data

Table 1 specifies the Input and Output Data of the Storage (AIH-STR) AIM. Links are to the Data Type specifications.

Table 1 – I/O Data of the Storage (AIH-STR) AIM

Input	Description
AIH Data Process Request	Request to Store AIH Data.
AIH Data	AIH Data to be Stored.
Output	**Description**
AIH Data Process Response	Response to Request to Store AIH Data.

7.1.9.4 JSON Metadata

https://schemas.mpai.community/AIH1/V1.0/AIMs/Storage.json

7.1.9.5 Conformance Testing

Table 2 provides the Conformance Testing Method for he Storag e(AIH-STR) AIM.

If a schema contains references to other schemas, conformance of data for the primary schema implies that any data referencing a secondary schema shall also validate against the relevant schema, if present and conform with the Qualifier, if present.

Table 2 – Conformance Testing Method for the Storage (AIH-STR) AIM

Receives	AIH Data Process Request	Shall validate against AIH Data Process schema.
	AIH Data	Shall validate against AIH Data schema.
Produces	AIH Data Process Response	Shall validate against AIH Data Process schema.

7.2 Reference Software

As a rule, MPAI provides Reference Software implementing the AI Modules released with the BSD-3-Clause licence and the following disclaimers:

1. The AIH-HSP V1.0 Reference Software Implementation, if in source code, is released with the BSD-3-Clause licence.

2. The purpose of this Reference Software is to provide a working Implementation of AIH-HSP V1.0, not to provide a ready-to-use product.
3. MPAI disclaims the suitability of the Software for any other purposes and does not guarantee that it is secure.
4. Use of this Reference Software may require acceptance of licences from the respective copyright holders. Users shall verify that they have the right to use any third-party software required by this Reference Software.

Note that at this stage AIH-HSP V1.0 does not provide Reference Software for AIMs.

7.3 Conformance Testing

An implementation of an AI Module conforms with AIH-HSP V1.0 if it accepts as input _and_ produces as output Data and/or Data Objects (the combination of Data of a Data Type and its Qualifier) conforming with those specified by AIH-HSP V1.0 for the AIM being tested for Conformance.

The Conformance is expressed by one of the two statements

1. "Data conforms with the relevant (Non-MPAI) standard" – for Data.
2. "Data validates against the Data Type Schema" – for Data Object.

The latter statement implies that:

1. Any Sub-Type of the Data conforms with the relevant Sub-Type specification of the applicable Qualifier.
2. Any Content and Transport Format of the Data conform with the relevant Format specification of the applicable Qualifier.
3. Any Attribute of the Data
    1. Conforms with the relevant (Non-MPAI) standard – for Data, or
    2. Validates against the Data Type Schema – for Data Object.

The method to Test the Conformance of an instance of Data or Data Object is specified in the *Data Types* chapter.

Note that at this stage the AIH-HSP V1.0 does not specify Conformance Testing for AIMs.

7.4 Performance Assessment

Performance is an umbrella term used to describe a variety of attributes – some specific of the application domain the Implementation intends to address. Therefore, Performance Assessment Specifications provide methods and procedures to measure how well an AIW or an AIM performs its function. Performance of an Implementation includes methods and procedures for all or a subset of the following characteristics:

1. Quality – for instance, how well a Face Identity Recognition AIM recognises faces, how precise or error-free are the changes in a Visual Scene detected by a Visual Change Detection AIM, or how satisfactory are the responses provided by an Answer to Multimodal Question AIW.
2. Robustness – for instance, how robust is the operation of an implementation with respect to duration of operation, load scaling, etc.
3. Extensibility – for instance, the degree of confidence a user can have in an Implementation when it deals with data outside of its stated application scope.
4. Bias: – for instance, how dependent on specific features of the training data is the inference, as in Company Performance Prediction when the accuracy of the prediction may widely change based on the size or the geographic position of a Company; or face recognition in Television Media Analysis.
5. Legality – for instance, in which jurisdictions the use of an AIM or an AIW complies with a regulation, e.g., the European AI Act.
6. Ethics: may indicate the conformity of an AIM or AIW to a target ethical standard.

Note that at this stage AIH-HSP V1.0 does not specify Performance Assessment for AIMs.

8 Data Types

8.1 Technical Specifications

This page gives the links to the specification of Data Types specified by ***Technical Specification: AI for Health (MPAI-AIH) - Health Secure Platform (AIH-HSP) V1.0***.

Acronym	AIH Name	JSON	Acronym	AIH Name	JSON
AIH-AHD	AIH Data	X	AIH-FDL	Federated Learn	X
AIH-DPR	AIH Data Process	X	AIH-HLD	Health Data	X
AIH-HPT	AIH Data Processing Type	X	AIH-LCF	Licence Confirm	X
AIH-AHT	AIH Taxonomies	X	AIH-MIO	Medical Imaging Object	X
AIH-ARD	ARA Data	X	AIH-MDL	Model Licence	X
AIH-ARQ	Audit	X	AIH-NSQ	Neurophysiological Signal Object	X
AIH-ECO	Behavioural Signal Object	X	AIH-OMO	Omics Object	X
AIH-BMD	Biometric Data	X	AIH-NSQ	Physiological Signal Object	X
AIH-BCL	Blockchain Licence	X	AIH-REG	Register	X
AIH-CRO	Clinical Record Object	X	AIH-TKN	Tokens	X
AIH-DIA	De-ID and Anonym	X	AIH-UPR	User Profile	X

8.1.1 AIH Data

8.1.1.1 Definition

AIH Data is data that a Front End produces by combining Health Data with a Model Licence. It may be processed locally and then sent to the Back End.

8.1.1.2 Functional Requirements

The life cycle of AIH Data is:

1. At the Health Front End, AIH Data
    1. Is passed through the Anomaly and Risk Alerting AIM.
    2. Is Stored in the Health Front End as AIH Data and may include any ARA Data.
    3. May be uploaded to the Health Back End.
2. At the Health Back End,

1. The Blockchain Licence ID is added to AIH Data.
2. The Licence is stored in the Blockchain as a smart contract.
3. Health Back End issues a Licence Confirm Request to the Blockchain.
4. If the Licence Confirm Response confirms that the requested Processing is included in the Licence, it retrieves AIH Data from the Secure Storage.
5. Performs the Processing.
6. Adds any ARA Data to the processed AIH Data.
7. Informs the User indicated by the End User.
8. Gets an ID for the Processed AIH Data.
9. Adds the Blockchain Licence ID to the Processed AIH Data.
10. Adds a label to AIH Data that has been De-Identified and/or Anonymised.
11. Stores the Processed AIH Data.

8.1.1.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/AIHData.json

8.1.1.4 Semantics

Label	Description
Header	AIH Data Header, Standard "AIH-AHD-Vx,y"
MInstanceID	Identifier of M-Instance.
UEnvironment	ID of Universe Environment.
AIHDataID	Identifier of AIH Data.
UserID	ID of End User producing this AIH Data instance.
AIHDataTime	Time of AIH Data.
AIHData	The actual AIH Data.
- HealthData	AIH Data Qualifier.
- ModelLicence	Model Licence as defined by End User
- SmartContractID	ID of Smart Contract produced by Blockchain.
- ARA Data	Anomaly & Risk Alerting Data
- De-IDAndAnonym	00= No De-IDAndAnonym; 01=Anonym; 10=De-ID; 11=Reserved.
- ParentAIHDataID	ID of AIH Data whose Processing has spawned this AIH Data.
DataXMData	Information about this AIH Data Instance.
DescrMetadata	Descriptive Metadata

8.1.1.5 Conformance Testing

A Data instance Conforms with AIH Data (AIH-AHD) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.

2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.2 AIH Data Process

8.1.2.1 Definition

A Data Type representing the payload of an AIH Data Process Request or Response:

1. The Request made to an AIH Processing AIM of an HFE or an HBE to process AIH Data.
2. The Response to the Request from an HFE or HBE AIH Processing AIM.

8.1.2.2 Functional Requirements

AIH Data Process Request includes:

1. AIH Data or AIH Data ID
2. Process Type
3. Tokens

AIH Process Response includes:

1. AIH Data or AIH Data ID
2. Process Status

8.1.2.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/AIHDataProcess.json

8.1.2.4 Semantics

Label	Description
Header	AIH Data Process Header "AIH-ADP-Vx.y"
MInstanceID	Identifier of M-Instance.
AIHDataProcessID	Identifier of Process Request.
AIHDataProcessTime	Time of Process Request.
UserID	ID of User.
AIHDataProcess	Data in AIH Data Process
- Request	If Request
- oneOf	one of
- AIHData	AIH Data
- AIHDataID	ID of AIH Data
- ProcessingType	Type of Process whose performance is requested.
- Tokens	Requesting User's Tokens
-Response	If Response
- oneOf	one of
- AIHData	AIH Data
- AIHDataID	ID of AIH Data

- ProcessingStatus	Boolean: 0=failure, 1=success
DataXMData	Information about this AIH Data Process Instance.
DescrMetadata	Descriptive Metadata

8.1.2.5 Conformance Testing

A Data instance Conforms with AIH Data Process (AIH-ADP if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.2.6 Performance Assessment

8.1.3 AIH Data Processing Type

8.1.3.1 Definition

AIH Data Processing Types primarily serve to express inference of an individual's health state. An AIH Data Processing Type identifies the kind of health state inferred from health data as a result of processing. The taxonomy applies to health data including behavioural, clinical, biological (omics), imaging, neurophysiological, and physiological data.

8.1.3.2 Functional Requirements

The Health Processing Type Taxonomy shall:

- Provide unique, stable identifiers for health-semantic processing types.
- Describe processing in terms of health state inference, not computation methods.
- Support both:
    - data-type-independent health inferences, and
    - data-type-specific health inferences where medically meaningful.
- Enable TFA components to:
    - declare which health inferences they perform,
    - declare which health inferences they support,
    - document which health inferences have been applied to data.
- Support extension with new processing types without breaking existing implementations.
- Provide identifiers that are:
    - human-readable,
    - machine-processable,
    - version-stable.
- Provide a single authoritative namespace for health processing type identifiers within TFA.

8.1.3.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/AIHDataProcessingType.json

8.1.3.4 Semantics

Label	Description

HealthStateDetection	Detection of the presence of a health-relevant state or condition.
HealthStateClassification	Classification of an individual into a health-relevant state or category.
HealthStateQuantification	Quantification of a health-relevant measure or parameter.
HealthStateCharacterisation	Derivation of characteristic properties of a health state.
HealthStateMonitoring	Assessment of the evolution of a health state over time.
HealthStatePrediction	Prediction of a future health state or outcome.
HealthPhenotypeDerivation	Derivation of a health phenotype from health data.
BehaviouralStateDetection	Detection of behaviour indicative of a health-relevant condition.
BehaviouralStateClassification	Classification of behavioural health states.
BehaviouralPatternCharacterisation	Characterisation of behavioural patterns relevant to health.
BehaviouralTrendMonitoring	Monitoring of behavioural changes over time.
BehaviouralRiskPrediction	Prediction of health risk based on behavioural data.
ClinicalConditionDetection	Detection of a clinical condition from clinical data.
ClinicalStateClassification	Classification of an individual's clinical state.
ClinicalOutcomeDerivation	Derivation of clinical outcomes or endpoints.
ClinicalPhenotypeDerivation	Derivation of a clinical phenotype.
ClinicalRiskAssessment	Assessment of clinical risk or prognosis.
MolecularVariantDetection	Detection of molecular or genomic variants.
MolecularProfileQuantification	Quantification of molecular expression profiles.
MolecularSignatureCharacterisation	Characterisation of molecular signatures.
BiomarkerStateDerivation	Derivation of health state through biomarkers.
MolecularRiskPrediction	Prediction of health risk based on molecular data.
AnatomicalStructureDetection	Detection of anatomical structures or anomalies.
PathologicalStateClassification	Classification of pathological imaging findings.
LesionExtentQuantification	Quantification of lesion or structural extent.
ImagingPhenotypeCharacterisation	Derivation of imaging-based phenotypes.
DiseaseProgressionMonitoring	Monitoring of disease evolution through imaging.
ImageDerivedRiskPrediction	Prediction of health risk from imaging features.
NeuralEventDetection	Detection of neurophysiological events.
BrainStateClassification	Classification of brain or cognitive states.
NeuroActivityQuantification	Quantification of neural activity measures.
NeuralPatternCharacterisation	Characterisation of neural patterns.
NeuroStateMonitoring	Monitoring of neurofunctional state over time.
NeurologicalRiskPrediction	Prediction of neurological health risk.
PhysiologicalEventDetection	Detection of physiological events.

PhysiologicalStateClassification	Classification of physiological health states.
PhysiologicalParameterQuantification	Quantification of physiological parameters.
PhysiologicalProfileCharacterisation	Characterisation of physiological profiles.
PhysiologicalTrendMonitoring	Monitoring of physiological trends.
PhysiologicalRiskPrediction	Prediction of health risk from physiological data.

8.1.3.5 Conformance Testing

A Data instance Conforms with AIH Data Processing (AIH-HPT) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.3.6 Performance Assessment

8.1.4 AIH Taxonomies

8.1.4.1 Definition

Taxonomies of various aspects related to IH Data.

8.1.4.2 Functional Requirements

Taxonomies cover:

1. AIH Data Classes
2. AIH Data Users
3. AIH Data Statuses
4. AIH Data Usages
5. Anonymisation/De-Identification Algorithms
6. Anomaly Types

8.1.4.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/AIHTaxonomies.json

8.1.4.4 Semantics

Label	Description
Header	AIH Taxonomies Header - Standard "AIH-HLT-V"
AIH Data Classes	The classes of Health data.
BehaviouralSignal	Observable human behavioural activity captured through sensors or digital interaction systems.
ClinicalRecord	Symbolic health information such as diagnoses, observations, procedures, medications, and laboratory results.
MedicalImaging	Spatially organised visual representations of anatomical or functional structures.
NeurophysiologicalSignal	Biosignals captured from neural or neuro-cognitive processes.

Omics	Molecular-level biological information derived from assays such as whole-genome sequencing, whole-exome sequencing, etc.
PhysiologicalSignal	Biosignals captured from physiological processes whose primary structure is a sampled temporal sequence representing time-series measurements acquired from sensors.
AIH Data Users	Different profiles of third-party users can affect the licensing of AIH Data Processing.
- End User	Individual who interacts with the AIH platform, primarily via a personal device, providing personal health data and receiving personalised data.
- Non-Profit Entity	Entity that is non-profit, e.g., a university.
- Profit Entity	Entity that is for profit, e.g., a pharmaceutical company.
- Clinical Entity	Entity that looks after the health of patients.
- Authorised Entity	Entity that has been authorised by an End User to process some of their AIH Data.
- Caregiver	Health providers that interact with the AIH-HSP to provide health and care services to specific End Users (nurses, caregivers, etc.) is folded into 2 intermediaries (back end and 3rd party).
AIH Data Status	In terms of Anonymised, Pseudonymised, Identified.
- Anonymised	AIH Data may be used if Anonymised.
- Pseudonymised	AIH Data may be used if Pseudonymised.
- Identified	AIH Data may be used for Identified End User.
AIH Data Usage	Types of authorised usage of AIH Data.
- Unrestricted	The processed data is open to public or semi-public consultation.
- Pseudonymised	The processed data may be published if End User identity are pseudonymised
- Anonymised	The processed data may be published if End User identity are anonymised
- Research	The processed data may be published if the publication is made on a journal to report research results.
- Patient use	The processed data may only be used by the patient or by individual authorised by the patient.
- Health care	The processed data may only be used by a Clinical Entity for health-related purpose in the Clinical Entity.
- Neurophysiological Signal Object	Spatially organised visual representations of anatomical or functional structures.

- Physiological Signal Object	Biosignals captured from physiological processes whose primary structure is a sampled temporal sequence representing time-series measurements
DeID & Anonym Algorithms	DeID&Anonymisation Algorithm.
- Data Masking	Replaces sensitive data with altered values while preserving the original data structure and format.
- Data Aggregation	Combines multiple data records into summary values to reduce individual data exposure.
- Generalisation	Substitutes specific data values with broader categories to reduce identifiability.
- Perturbation	Introduces controlled modifications or noise into data to prevent accurate inference of original values.
- Tokenisation	Replaces sensitive data with surrogate tokens, with original values stored in a secure mapping.
- Hashing	Applies a one-way cryptographic transformation that prevents recovery of the original data.
- Removal of Identifiers	Deletes direct identifiers from a dataset to reduce the likelihood of re-identification.
- K-Anonymity	Ensures each record is indistinguishable from at least *k–1* others based on quasi-identifiers.
- L-Diversity	Ensures that multiple distinct sensitive values exist within each k-anonymous group.
- Differential Privacy	Provides formal guarantees by limiting the influence of any single data subject through calibrated noise.
- Synthetic Data Generation	Produces artificial data exhibiting statistical similarity to real data without representing real individuals.
- Homomorphic Encryption	Enables computation on encrypted data and returns encrypted results without plaintext exposure.
Risk	Risks classified according to Manchester Protocol.
- Red	Emergency. Indicates critical situations that require immediate attention.
- Orange	Very urgent. Patients who need quick attention but whose condition is not immediately life-threatening.
- Yellow	Urgent. Indicates that the patient needs care, but the condition is not serious.
- Green	Less urgent. Patients with less severe conditions that can wait a bit longer for care.

- Blue	Non-urgent. Patients whose conditions are not urgent and can wait for care.	
AIH Data Anomalies	Classes of alert messages caused by anomalies in health	
	Definition	**Anomaly examples**
- Point Anomaly	Individual data points that deviate significantly from the rest of the dataset	Sudden spikes in heart rate or blood pressure readings.
- Contextual Anomaly	Anomalous data points that in a specific context - may be normal in another.	Elevated heart rate during sleep versus during exercise.
- Collective Anomaly	A set of related data points that collectively deviate from the expected pattern.	A series of abnormal ECG readings indicating a potential cardiac event.
- Medical Condition Anomaly	Abnormalities in patient data due to medical conditions.	Seizures, falls, arrhythmias, atrial fibrillation, ventricular tachycardia.
- Erroneous Data Anomaly	Data errors that may be due to faults or malicious attacks.	Anomaly in - Biorhythm signals (e.g., heartbeat anomalous patterns, respiratory anomalous patterns). - Multimodal patterns (diverse data sources show conflicting patterns).

8.1.5 AIH Data

8.1.5.1 Definition

Data describing anomaly in and risk from AIH Data.

8.1.5.2 Functional Requirements

ARA Data includes

1. AIH Data ID
2. Anomaly (per Taxonomy)

8.1.5.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/ARAData.json

8.1.5.4 Semantics

Label	Description
Header	ARA Data Header - Standard "AIH-ARD-Vx.y"
MInstanceID	Identifier of M-Instance.

UEnvironmentID	Identifier of U-Environment.
ARADataID	Identifier of ARA Data.
ARADataTime	Time of ARA Data.
UserID	Id of User.
ARAData	Data in ARA Data.
- AIHDataID	ID of AIH Data with Anomaly and/or Risk.
- Anomalies[]	Set of Anomalies.
- Anomaly	A specific Anomaly.
- Risk	One of • **Red**: Immediate care required (emergent). • **Orange**: Very urgent care needed. • **Yellow**: Urgent care required. • **Green**: Not urgent. • **Blue**: Non-urgent.
DataXMData	Information about this ARA Data Instance.
DescrMetadata	Descriptive Metadata.

8.1.5.5 Conformance Testing

A Data instance Conforms with ARA Data (AIH-ARD) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.6 Audit

8.1.6.1 Definition

The Request to the Auditing AIM to Audit the Processing of AIH Data or the Response from the Auditing AIM.

8.1.6.2 Functional Requirements

Audit Request includes:

1. User ID
2. Time
3. Processing Types for which infringement is sought.

Audit Response includes a list of

1. AIH Data ID
2. Time of Processing
3. AIM performing infringing Processing

8.1.6.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/Audit.json

8.1.6.4 Semantics

Label	Description
Header	Audit Header - Standard "AIH-ADT-Vx.y"
MInstanceID	Identifier of M-Instance.
AuditID	Identifier of Audit Request.
AuditTime	Time of Audit Request.
Audit	Data in Audit
- Request	If Request
- UserID	ID of User for which Audit is requested.
- AuditPeriod	Period of time for which Audit is requested.
- Processing Types	For which infringement is sought.
- Response	If response
- AIHData[]	Data of the set of Affected AIH Data IDs.
- ProcessingTypes[]	Set of Processing performed.
- AIMInstance	ID of AIM that performed the infringing Processing.
- ProcessTime	Date of infringing Processing.
- AIHDataID	AIH Data affected by infringing Processing.
DataXMData	Information about this AIH Data Instance.
DescrMetadata	Descriptive Metadata

8.1.6.5 Conformance Testing

A Data instance Conforms with Audit (AIH-ADT) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.7 Behavioural Signal Object

8.1.7.1 Definition

Behavioural Signal Object includes:

Behavioural Signal Data representing observable human behavioural activity captured through sensors or digital interaction systems, whose primary structure is a sampled temporal sequence or event-based record describing motor, gestural, facial, interaction, or other externally measurable behavioural patterns. These signals may be continuous or discretely sampled waveforms, multichannel motion trajectories, event logs, or interaction traces, accompanied by metadata describing the acquisition conditions, sensor characteristics, and timing information.

Behavioural Signal Qualifier specified by MPAI-TFA, providing information about the Sub-Types, Formats, and Attributes of the Behavioural Signal Data

8.1.7.2 Functional Requirements

Behavioural Signal Object shall satisfy the following requirements:

1. **Behavioural Signal Object Header** The Behavioural Signal Object shall include a header identifying the version of the Behavioural Signal Object standard.
2. **Behavioural Signal Object Identification** The Behavioural Signal Object shall include an identifier uniquely referencing the Behavioural Signal Object.
3. **End User Identification** The Behavioural Signal Object shall include the identifier of the End User the Behavioural Signal Data refers to.
4. **Time Information** The Behavioural Signal Object shall include the time information associated with the Behavioural Signal Data.
5. **Behavioural Signal Data** The Behavioural Signal Object shall include Behavioural Signal Data per the Behavioural Signal Qualifier.
6. **Behavioural Signal Qualifier** The Behavioural Signal Object shall include a Behavioural Signal Qualifier describing the Behavioural Signal Data.
7. **Traceability** The Behavioural Signal Object shall include provenance information and time of production.
8. **Descriptive Metadata** The Behavioural Signal Object shall include descriptive metadata.

8.1.7.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/BehaviouralSignalObject.json

8.1.7.4 Semantics

Label	Description
Header	Behavioural Signal Object Header – Standard "AIH-BSO-Vx.y".
BehaviouralSignalObjectID	Identifier of the Behavioural Signal Object.
EndUserID	ID of the End User the Behavioural Signal Data refers to.
BehaviouralSignalObjectTime	Time information of the Behavioural Signal Data.
BehaviouralSignalData	Behavioural Signal Data per Qualifier.
BehaviouralSignalQualifier	Behavioural Signal Qualifier.
DataXMData	Information about this Behavioural Signal Object Instance.
DescrMetadata	Descriptive Metadata.

8.1.7.5 Conformance Testing

A Data instance Conforms with Behavioural Signal Object (AIH-BSO) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.8 Biometric Data

8.1.8.1 Definition

Biometric Data is a Data Type including characteristics of a human body.

8.1.8.2 Functional Requirements

Biometric Data includes

1. HeartRate
2. HeartRateVariability
3. BrainState
4. GalvanicSkinResponse
5. MyoelectricIntensity
6. SkinTemperature

8.1.8.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/BiometricData.json

8.1.8.4 Semantics

Label	Description
Header	Biometric Data Header - Standard "AIH-BMC-Vx.y"
MInstanceID	Identifier of M-Instance.
UEnvironmentID	Identifier of Universe Environment.
BiometricDataID	Identifier of Biometric Data.
BiometricData	Time info of Biometric Data.
UserID	ID of User whose Biometric Data are collected.
HeartRate	Data per ECG Qualifier.
HeartRateVariability	Data per ECG Qualifier.
BrainState	Data per EEG Qualifier.
GalvanicSkinResponse	Measure of changes in skin conductivity expressed in micro-Siemens (μS).
MyoelectricIntensity	Myoelectric signals measured in milli-Volt (mV).
SkinTemperature	Measured in Degrees Celsius.
DataXMData	Information about this Biometric Data Instance.
DescrMetadata	Descriptive Metadata

8.1.8.5 Conformance Testing

A Data instance Conforms with Biometric Data (AIH-BMC) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.9 Blockchain Licence

8.1.9.1 Definition

The Request made to the Blockchain to Store a Model Licence as a Smart Contract and to provided the Smart Contract (Blockchain Licence) ID.

8.1.9.2 Functional Requirements

Blockchain Licence Request includes:

1. Model Licence

2. Tokens

Blockchain Licence Response includes

1. Smart Contract (Blockchain Licence) ID.
2. Blockchain Licence State

8.1.9.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/BlockchainLicence.json

8.1.9.4 Semantics

Label	Description
Header	Blockchain Licence Header - Standard "AIH-BLL-Vx.y"
MInstanceID	Identifier of M-Instance.
BlockchainLicenceID	Identifier of Blockchain Licence.
BlockchainLicenceTime	Time of Blockchain Licence.
BlockchainLicence	Data in Blockchain Licence.
- Request	If Request
- ModelLicence	End User's Model Licence.
- Tokens	EndUser's Tokens
- Response	If Response
- SmartContractID	ID of Smart Contract
- BlockchainLicenceStatus	Boolean; 0=failure, 1= success
DataXMData	Information about this AIH Data Instance.
DescrMetadata	Descriptive Metadata

8.1.9.5 Conformance Testing

A Data instance Conforms with Blockchain Licence (AIH-BLL) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.10 Clinical Record Object

8.1.10.1 Definition

Clinical Record Object specifies the representation of structured, symbolic health information such as diagnoses, observations, procedures, medications, and laboratory results and represents discrete clinical facts rather than continuous signals and are intended to support AI-based reasoning, decision support, and integration with signal-based health data. It references Clinical Record Qualifier.

8.1.10.2 Functional Requirements

A Clinical Record Object shall enable:

- Representation of structured clinical information using symbolic values.
- Association of clinical facts with time, subject, and clinical context.
- Integration with AI-based reasoning, decision support, and analytics.
- Interoperability with signal-based and imaging-based health data.

A Clinical Record Object shall:

- Support standard clinical vocabularies and taxonomies.
- Allow partial or incremental clinical information.
- Remain independent of any specific electronic health record (EHR) system.

8.1.10.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/ClinicalRecordObject.json

8.1.10.4 Semantics

Label	Description
Header	Clinical Records Object Header – Standard "TFA-CRO-Vx.y".
ClinicalRecordObjectID	Identifier of the Clinical Record instance.
ClinicalRecordObjectTime	Time associated with the clinical record entry.
RecordType	Type of clinical record (e.g. Diagnosis, Observation, Procedure, Medication, LabResult).
ClinicalRecordObjectData	Symbolic clinical data payload.
ClinicalRecordQualifier	Qualifier defining coding system, interpretation, or clinical scope.
DataXMData	Information about this Clinical Records Object Instance.
DescrMetadata	Descriptive Metadata

8.1.10.5 Conformance Testing

A Data instance Conforms with Clinical Records Object (AIH-CRO) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.11 De-ID and Anonym

8.1.11.1 Definition

The Request to the De-Identification & Anonymisation AIM to de-identify or anonymise AIH Data or the Response from the De-Identification & Anonymisation AIM.

8.1.11.2 Functional Requirements

The De-ID and Anonym Request includes:

1. AIH Data ID
2. DeIDAndAnonymType
3. DeIDAndAnonymAlgoID

The De-ID and Anonym Response includes

1. De-ID and Anonym'd AIH Data ID
2. Processing State.

8.1.11.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/DeIDAndAnonym.json

8.1.11.4 Semantics

Label	Description
Header	De-ID and Anonym Header - Standard "AIH-DIA-Vx.y"
MInstanceID	Identifier of M-Instance.
DeIDAndAnonymID	Identifier of DIA Request.
DeIDAndAnonymTime	Time of DIA Request.
DeIDAndAnonym	Data in De-ID and Anonym
- Request	If Request
- AIHDataID	ID of AIH Data.
- DeIDAndAnonymType	00=reserved; 01=De-Identify;10=Anonymise; 11= both De-Identify and Anonymise.
- DeIDAndAnonymAlgoID	ID of DeIDAndAnonym algorithm.
- Response	If Response
- AIH Data ID	De-ID and Anonym'd AIH Data ID.
- ProcessingState	0=Failure; 1=Success
DataXMData	Information about this De-ID and Anonym Instance.
DescrMetadata	Descriptive Metadata

8.1.11.5 Conformance Testing

A Data instance Conforms with De-ID and Anonym (AIH-DIA) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.12 Federated Learn

8.1.12.1 Definition

The Request to a Health Front End to provide its trained NN Model or the Response from the Health Front End.

8.1.12.2 Functional Requirements

The Federated Learn Request includes

1. Health Front End ID
2. ID of NN Model before it is subjected to Machine Learning.(Pre-Learn)

The Federated Learn Response includes

1. NN Model after it has been subjected to Machine Learning (Post-Learn).

8.1.12.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/FederatedLearn.json

8.1.12.4 Semantics

Label	Description
Header	Federated Learn Header - Standard "AIH-FDL-Vx.y"
MInstanceID	Identifier of M-Instance.
FederatedLearnID	Identifier of Federated Learn.
FederatedLearnTime	Time of Federated Learn.
FederatedLearn	Data in Federated Learn.
- Request	If Request
- HFEID	ID Of Health Front End
- PreLearnNNModelID	ID of NN Model downloaded from the MPAI Store.
- Response	If Response
- PostLearnNNModel	NN Model after Machine Learning.
DataXMData	Information about this Federated Learn Instance.
DescrMetadata	Descriptive Metadata

8.1.12.5 Conformance Testing

A Data instance Conforms with Federated Learn (AIH-FDL) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.13 Health Data

8.1.13.1 Definition

Health Data is End User's Data received by a Health Front End from a Health Device.

8.1.13.2 Functional Requirements

Health Data belongs to one of Health Data types listed in the Qualifiers.

8.1.13.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/HealthData.json

8.1.13.4 Semantics

Label	Description
Header	Health Data Header, Standard "AIH-HLD-Vx.y"
MInstanceID	Identifier of M-Instance.
HealthDataID	Identifier of Health Data.
HealthDataTime	Time of Health Data.
HealthObject	Set of Health Data.
- Data	The Health Data.
- Qualifier	Health Data Qualifier.
DataXMData	Information about this Health Data Instance.
DescrMetadata	Descriptive Metadata

8.1.13.5 Conformance Testing

A Data instance Conforms with Health Data (AIH-HLD) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.14 Licence Confirm

8.1.14.1 Definition

The request to the Blockchain to confirm that an Process Type performed on AIH Data of a given ID conforms with the Blockchain Licence with a given Licence ID or the response to the Licence Confirm Request.

8.1.14.2 Functional Requirements

Licence Confirm Request includes:

1. AIH Data ID
2. Process Type
3. Intended time of Process.

Licence Confirm Response includes

1. Boolean: 0=Process infringes, 1=Process complies.

8.1.14.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/LicenceConfirm.json

8.1.14.4 Semantics

Label	Description
Header	Licence Confirm Header - Standard "AIH-LCF-Vx.y"
MInstanceID	Identifier of M-Instance.
LicenceConfirmID	Identifier of Licence Confirm.

LicenceConfirmTime	Time of Licence Confirm.
LicenceConfirm	Data in Licence Confirm.
- Request	If Request
- AIHDataID	ID of AIH Data
- ProcessType	Process Type
- Time	Intended Process Execution Time
- Response	Boolean: 0=Process infringes, 1=Process complies.
DataXMData	Information about this Licence Confirm Instance.
DescrMetadata	Descriptive Metadata

8.1.14.5 Conformance Testing

A Data instance Conforms with Licence Confirm (AIH-LCF) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.15 Medical Imaging Object

8.1.15.1 Definition

Medical Imaging Object represents spatially organised visual representations of anatomical or functional structures and is intended to support AI-based analysis, interpretation, and fusion with other health data types. It references Medical Imaging Qualifier.

8.1.15.2 Functional Requirements

A Medical Imaging Object shall enable:

- Representation of medical image data independent of acquisition device vendor.
- Support for single images, image series, and volumetric datasets.
- Association of image data with acquisition time and modality.
- Integration with AI-based image analysis and inference pipelines.
- Interoperability with non-imaging health data (e.g. physiological or genomic data).

A Medical Imaging Object shall be:

- Modality-agnostic.
- Compatible with both 2D and 3D image data.
- Suitable for offline and real-time AI processing.

8.1.15.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/MedicalImagingObject.json

8.1.15.4 Semantics

Label	Description
Header	Medical Imaging Object Header – Standard “TFA-MIO-Vx.y”.
MedicalImagingObjectID	Identifier of the Medical Imaging data instance.

MedicalImagingObjectTime	Time of image acquisition.
ImagingModality	Imaging modality (e.g. CT, MRI, X-ray, Ultrasound, PET).
MedicalImagingObjectData	Image data payload (single image, image series, or volume).
SpatialMetadata	Information describing spatial resolution, orientation, and scale.
MedicalImagingQualifier	Qualifier describing image encoding, format, and interpretation constraints.
DataXMData	Information about this Medical Imaging Object Instance.
DescrMetadata	Descriptive metadata.

8.1.15.5 Conformance Testing

A Data instance Conforms with Medical Imaging Object (AIH-MIO) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.16 Model Licence

8.1.16.1 Definition

Data representing the AIH Data Licence that a Health Front End sends to the Health Back End.

8.1.16.2 Functional Requirements

The Model Licence contains

- End User ID
- Model Licence ID
- AIH Data ID
- Date of issuance of the Model Licence by the End User.
- AIH Data Taxonomy element identification.
- Licensing terms to Back End:
    - Duration of Model Licence.
    - Processing types, according to Taxonomy of AI Module types.
    - Usage of results based on Taxonomy of Classes of processing result usages.
- Sub-licensing Terms to Third-Party Users:
    - Duration of Licence.
    - Classes of Third-Party users according to Taxonomy.
    - Processing types according to Taxonomy of AI Module Processing types.
    - Usage of results based on Taxonomy of Classes of processing result usages.

8.1.16.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/ModelLicence.json

8.1.16.4 Semantics

Label	Description
Header	Model Licence Header - Standard "AIH-MDL-Vx.y"
ModelLicenceID	Identifier of Model Licence.

EndUserID	Identifier of End User the AIH Data refers to.
AIHDataID	Identifier of AIH Data.
AIHDataType	Type of AIH Data based on Taxonomy.
ModelLicenceTime	Start time and end time of Model Licence validity.
ModelLicenceData	Data in Model Licence.
BackEndLicence	If Back End
- EndUserID	ID of End User producing the Model Licence.
- BackendID	ID of Back End the Model Licence is sent to.
- AIHDataID	ID issued by end user. New ID issued for the processed AIHData.
- AIHDataStatus	One of Identified, Anonymised, Pseudonymised.
- AIHDataProcess	Types of Processing applicable to unprocessed and already processed AIHData.
- AIHDataUsage	Types of Result Usage.
ThirdPartyUserLicence	If Third Party User
- BackendID	ID of Back End re-issuing the Model Licence.
- ThirdPartyUserID	ID of Third Party being licensed.
- LicensableEndUsers[]	IDs of specific End Users that may be licenced.
- UserID	ID of licensable User.
- AIHDataClasses[]	Licensable AIH Data Classes.
- AIHDataID	ID issued by end user. New ID issued for the processed AIH Data.
- Time	Start time and end time of licence validity.
- UserTypes	Classes of Users authorised to use Processing Results.
- ProcessTypes	Types of Processing applicable to unprocessed or already processed AIHData.
- AnomalyTypes	Types of Anomaly that may be encountered during AIH Data Processing.
- UsageTypes	Types of Result Usage
DataXMData	Information about this Model Licence Instance.
DescrMetadata	Descriptive Metadata

8.1.16.5 Conformance Testing

A Data instance Conforms with Model Licence (AIH-MDL) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.

2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.17 Neurophysiological Signal Object

8.1.17.1 Definition

Neurophysiological Signal Object includes:

1. **Neurophysiological Signal Data** representing biosignals captured from **neural or neuro-cognitive processes** whose primary structure is a sampled temporal sequence representing time-series measurements acquired from sensors that capture **neural, magnetic, optical, or ocular activity** of the human brain or nervous system. These signals are typically continuous or discretely sampled waveforms, possibly multichannel, accompanied by metadata describing the acquisition conditions, sensor characteristics, and timing information.
2. **Neurophysiological Signal Qualifier** specified by **MPAI-TFA**, providing information about the **Sub-Types**, **Formats**, and **Attributes** of the Neurophysiological Signal Data.

8.1.17.2 Functional Requirements

Neurophysiological Signal Data satisfies all the following requirements:

1. **Time-Series Structure:** The data consists of one or more sequences of samples ordered in time.
2. **Neurophysiological Origin:** The measured signal reflects a neurophysiological process (e.g., electrical, magnetic, optical, or ocular activity associated with brain or neural function).
3. **Information:** The data includes or is associated with sampling metadata (e.g., sampling rate, units, channel count).
4. **Sensor-Based Acquisition:** The signal is obtained from a physical sensor or neurophysiological acquisition device (e.g., EEG electrodes, MEG magnetometers, fNIRS optodes, eye-tracking sensors).
5. **Channel Semantics:** Each channel corresponds to a defined neurophysiological measurement (e.g., EEG electrode, MEG sensor, fNIRS source-detector pair, eye-tracking axis).
6. **Acquisition Metadata:** The data includes metadata describing the recording context (e.g., device, subject, start time, optional annotations).

8.1.17.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/NeurophysiologicalSignalObject.json

8.1.17.4 Semantics

Label	Description
Header	Neurophysiological Signal Object Header – Standard "AIH-NSO-Vx.y".
NeurophysiologicalSignalObjectID	Identifier of the Neurophysiological Signal Object.
EndUserID	ID of the End User the Neurophysiological Signal Data refers to.
NeurophysiologicalSignalObjectTime	Time information of the Neurophysiological Signal Data.
NeurophysiologicalSignalData	Neurophysiological Signal Data per Qualifier.
NeurophysiologicalSignalQualifier	Neurophysiological Signal Qualifier.

Label	Description
DataXMData	Information about this Neurophysiological Signal Object Instance.
DescrMetadata	Descriptive Metadata.

8.1.17.5 Conformance Testing

A Data instance Conforms with Neurophysiological Signal Object (AIH-NSO) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.18 Omics Object

8.1.18.1 Definition

Genomics Omics Object includes:

Omics Data representing molecular-level biological information derived from assays such as whole-genome sequencing, whole-exome sequencing, targeted sequencing, RNA-seq, proteomics, metabolomics, methylation arrays, or other high-throughput omics technologies. The primary structure may be variant-level data (e.g., VCF records), read-level files (e.g., FASTQ/BAM), feature matrices (e.g., gene-expression tables), or molecular profiles (e.g., proteomic or metabolomic abundance tables), accompanied by metadata describing sample preparation, assay technology, reference genome/build, processing pipelines, and quality metrics. Omics Qualifier specified by MPAI-TFA, providing information about the Sub-Types, Formats, and Attributes of the Genomics Omics Data.

8.1.18.2 Functional Requirements

Omics Object shall satisfy the following requirements:

- **Omics Object Header:** The Omics Object shall include a header identifying the version of the Genomics Omics Object standard.
- **Omics Object Identification:** The Omics Object shall include an identifier uniquely referencing the Genomics Omics Object.
- **End User Identification:** The Omics Object shall include the identifier of the End User the Genomics Omics Data refers to.
- **Time Information:** The Omics Object shall include the time information associated with the Genomics Omics Data.
- **Omics Data:** The Omics Object shall include Genomics Omics Data per the Genomics Omics Qualifier.
- **Omics Qualifier:** The Omics Object shall include a Genomics Omics Qualifier describing the Genomics Omics Data.
- **Traceability:** The Omics Object may include provenance information and time of production.

8.1.18.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/OmicsObject.json

8.1.18.4 Semantics

Label	Description
Header	Omics Object Header – Standard "AIH-OMO-Vx.y".
OmicsObjectID	Identifier of the Omics Object.
EndUserID	ID of the End User the Omics Data refers to.
OmicsObjectTime	Time information of the Omics Data.
OmicsData	Omics Data per Qualifier.
OmicsQualifier	Omics Qualifier.
DataXMData	Information about this Omics Object Instance.
DescrMetadata	Descriptive Metadata.

8.1.18.5 Conformance Testing

A Data instance Conforms with Omics Object (AIH-OMO) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.19 Physiological Signal Object

8.1.19.1 Definition

Physiological Signal Object includes:

1. Physiological Signal Data representing biosignals captured from physiological processes whose primary structure is a sampled temporal sequence representing time-series measurements acquired from sensors that capture physiological activity of the human body. These signals are typically continuous or discretely sampled waveforms, possibly multichannel, accompanied by metadata describing the acquisition conditions, sensor characteristics, and timing information.
2. Physiological Signal Qualifier specified by MPAI-TFA providing information about the Sub-Types, Formats and Attributes of the Physiological Signal Data.

8.1.19.2 Functional Requirements

Physiological Signal Data satisfies all the following requirements::

1. **Time-Series Structure** The data consists of one or more sequences of samples ordered in time.
2. **Physiological Origin** The measured signal reflects a physiological process (e.g., cardiac, muscular, ocular, respiratory, vascular, electrodermal).
3. **Sampling Information** The data includes or is associated with sampling metadata (e.g., sampling rate, units, channel count).
4. **Sensor-Based Acquisition** The signal is obtained from a physical sensor or biosignal acquisition device.
5. **Channel Semantics** Each channel corresponds to a defined physiological measurement (e.g., ECG lead, EMG electrode, airflow sensor).
6. **Acquisition Metadata** The data includes metadata describing the recording context (e.g., device, subject, start time, optional annotations).

8.1.19.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/PhysiologicalSignalObject.json

8.1.19.4 Semantics

Label	Description
Header	Physiological Signal Object Header - Standard "AIH-PSO-Vx.y"
PhysiologicalSignalObjectID	Identifier of the ECG Object.
EndUserID	ID of End User the ECG Data refers to.
PhysiologicalSignalObjectTime	Time info of ECG Data.
PhysiologicalSignalData	ECG Data per Qualifier.
PhysiologicalSignalQualifier	ECG Qualifier.
DataXMData	Information about this Physiological Signal Object Instance.
DescrMetadata	Descriptive Metadata

8.1.19.5 Conformance Testing

A Data instance Conforms with Physiological Signal Object (AIH-PSO) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.20 Register

8.1.20.1 Definition

Register Request is a Data Type that a User employs to Register with the Health Back End directly - if a Third Party User - or via a Health Front End - if an End User.
Register Response is the Health Back End response to the Register Request.

8.1.20.2 Functional Requirements

Request includes:

1. User Profile

Response includes:

1. Yes/No response
2. Registration Token.

8.1.20.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/Register.json

8.1.20.4 Semantics

Label	Description
Header	Register Header, Standard "AIH-REG-Vx.y"
MInstanceID	Identifier of M-Instance.
RegisterID	Identifier of Register.

RegisterTime	Time of Registration
RegisterData	Set of Register Data.
- Request	Data included in the Request.
- UserProfile	User Profile.
- RequestedServices	List of Services for which access is requested.
- Response	Data include in the Response.
- Success	Registration outcome (boolean, 0=failure)
- Tokens	Tokens enabling Registering User to access the corresponding Services.
DataXMData	Information about this Register Instance.
DescrMetadata	Descriptive Metadata

8.1.20.5 Conformance Testing

A Data instance Conforms with Register (AIH-REG) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.21 Tokens

8.1.21.1 Definition

Tokens are Service-specific Data provided by the Back End to a User who registers with the Back End to enable the User to access specific Services.

8.1.21.2 Functional Requirements

The Token allows access to one or more of the following Services accessible to a User:

1. Data Storage
2. Licence Change
3. DIA
4. Data Processing
5. Auditing

8.1.21.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/Tokens.json

8.1.21.4 Semantics

Label	Description
Header	Tokens Header, Standard "AIH-TKN-Vx.y"
- Standard-Tokens	The characters
- Version	Major version – 1 or 2 characters
- Dot-separator	The character .

- Subversion	Minor version – 1 or 2 characters
MInstanceID	Identifier of M-Instance.
UserID	Identifier of User.
TokensID	Identifier of Tokens.
TokensTime	Time info of Tokens.
Tokens	Tokens Data.
- ServiceTypes[]	List of Service Types for which Tokens are available.
DataXMData	Information about this Tokens Instance.
DescrMetadata	Descriptive Metadata

8.1.21.5 Conformance Testing

A Data instance Conforms with Token (AIH-TKN) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.1.22 User Profile

8.1.22.1 Definition

User Profile includes all data required for Registration with a Health Back End.

8.1.22.2 Functional Requirements

When the User is an individual, the User Profile includes the following:

1. Name
2. Surname
3. User Type
4. Address
5. Age
6. Country

When the User is an Organisation, the User Profile includes the following

1. Name
2. Code
3. Address
4. Country
5. Type

8.1.22.3 Syntax

https://schemas.mpai.community/AIH1/V1.0/data/UserProfile.json

8.1.22.4 Semantics

Label	Description
Header	User Profile Header, Standard "AIH-UPR-Vx.y"

MInstanceID	Identifier of M-Instance.
UserProfileID	Identifier of User Profile.
UserProfileTime	Time info of User Profile.
UserProfileData	User Profile Data.
- IfHuman	If human.
- Name	Name
- Surname	Surname
- Birthday	Date of birth
- Address	Residence address.
- Country	Nationality
- IfOrganisation	If organisation
- Name	Organisation name
- Code	Code of business register
- Address	Official address
- Country	Country of official address
- Type	Type per Taxonomy
DataXMData	Information about this User Profile Instance.
DescrMetadata	Descriptive Metadata

8.1.22.5 Conformance Testing

A Data instance Conforms with User Profile (AIH-UPR) if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas.

8.2 Conformance testing

The Conformance a Data instance conforms with AIH-HSP V1.0 is expressed by one of the two statements:

1. "Data conforms with the relevant (Non-MPAI) standard" – for Data.
2. "Data validates against the Data Type Schema" – for Data Object.

The latter statement implies that:

A Data instance Conforms with AIH-HSP V1.0 specified Data Type if:

1. Its JSON Object validates against its JSON Schema.
2. Any included JSON Object validates against its JSON Schema.
3. All Data in the JSON Object:
    1. Have the specified Data Types.
    2. Conform with the Qualifiers signaled in their JSON Schemas. For example, if the data cldata to be UNICODE, it should conform with what the Text Qualifier (MPAI-TFA V1.4) defines as UNICODE.

Note that at this stage the AIH-HSP V1.0 does specifies Conformance Testing for Data Types.

8.3 Performance Assessment

Performance is an umbrella term used to describe a variety of attributes – some specific of the application domain served by a specific Data Type. Therefore, Performance Assessment Specifications provide methods and procedures to measure how well a Data instance represents an original Data entity. Performance of an Implementation includes methods and procedures for all or a subset of the following characteristics:

1. Quality– for example, how well a Scene Descriptors instance represent a scene.
2. Bias: – for example, how dependent on specific features of the training data is the inference represented by the Data instance.
3. Legality– for example, whether the Data instance was produced in a jurisdiction at a time by an AIM that complies with the relevant a regulation, e.g., the European AI Act.
4. Ethics – for example, the data instance complies to a target ethical standard.

Note that at this stage the AIH-HSP V1.0 specifies Performance Assessment only of some Data Types.