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

**Public document**

|  |  |
| --- | --- |
| **N740** | 2022/06/22 |
| **Source** | Requirements (AIH) |
| **Title** | Initial MPAI-AIH Architecture |
| **Target** | MPAI Members |

# Abstract

Artificial Intelligence for Health data (MPAI-AIH) is an MPAI project addressing the secure collection, AI-based processing and secure access to Health data[[1]](#footnote-1).

Contents

[Abstract 1](#_Toc106466023)

[1 Introduction (Informative) 1](#_Toc106466024)

[2 AI Health Secure Platform 2](#_Toc106466025)

[2.1 Actors 3](#_Toc106466026)

[2.2 Services 3](#_Toc106466027)

[2.3 APIs 4](#_Toc106466028)

[3 Healthcare use case 4](#_Toc106466029)

[3.1 User health data collection 4](#_Toc106466030)

[3.2 Access to healthcare data 4](#_Toc106466031)

[4 Federated Services 5](#_Toc106466032)

[4.1 Federated Learning Mobile applications 5](#_Toc106466033)

[4.2 Healthcare Application Use Case 5](#_Toc106466034)

[4.3 Federated Learning Processes 5](#_Toc106466035)

[4.3.1 Training process 6](#_Toc106466036)

[4.3.2 Inference Process 6](#_Toc106466037)

[4.4 MPAI-AIH Federated Components 6](#_Toc106466038)

[5 References 6](#_Toc106466039)

# Introduction (Informative)

In recent years, Artificial Intelligence (AI) and related technologies have been applied to a broad range of applications, have started affecting the life of millions of people and are expected to do so even more in the future. As digital media standards have positively influenced industry and billions of people, so AI-based data coding standards are expected to have a similar positive impact. Indeed, research has shown that data coding with AI-based technologies is generally *more efficient* than with existing technologies for, e.g., compression and feature-based description.

However, some AI technologies may carry inherent risks, e.g., in terms of bias toward some classes of users. Therefore, the need for standardisation is more important and urgent than ever.

The international, unaffiliated, not-for-profit MPAI – Moving Picture, Audio and Data Coding by Artificial Intelligence Standards Developing Organisation has the mission to develop *AI-enabled data coding standards*. MPAI Application Standards enable the development of AI-based products, applications and services.

As a part of its mission, MPAI has developed standards operating procedures to enable users of MPAI implementations to make informed decision about their applicability. Central to this is the notion of Performance, defined as a set of attributes characterising a reliable and trustworthy implementation.

For the aforementioned reasons, to fully achieve the MPAI mission, Technical Specifications must be complemented by an ecosystem designed, created and managed to underpin the life cycle of MPAI standards through the steps of specification, technical testing, assessment of product safety and security, and distribution.

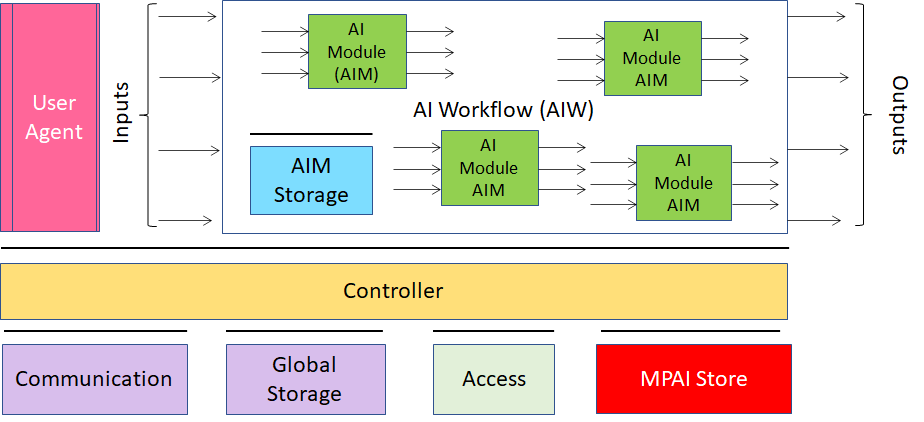
In the following, Terms beginning with a capital letter are defined in *Table 1* if they are specific to this Standard and in *Table 2* if they are common to all MPAI Standards.

The MPAI Ecosystem is fully specified in [1]. It is composed of:

* MPAI as provider of Technical, Conformance and Performance Specifications.
* Implementers of MPAI standards.
* MPAI-appointed Performance Assessors.
* The MPAI Store which takes care of secure distribution of validated Implementations.

*Figure 1* depicts the MPAI-AIF Reference Model under which Implementations of MPAI Applic­ation Standards and user-defined MPAI-AIF conforming applications operate.

An AIF Implementation allows execution of AI Workflows (AIW), composed of basic processing elements called AI Modules (AIM).



*Figure 1 – The AI Framework (AIF) Reference Model and its Components*

MPAI Application Standards normatively specify Syntax and Semantics of the input and output data and the Function of the AIW and the AIMs, and the Connections between and among the AIMs of an AIW.

In particular, an AIM is defined by its Function and data, but not by its internal architecture, which may be based on AI or data processing, and implemented in software, hardware or hybrid software and hardware technologies.

MPAI defines Interoperability as the ability to replace an AIW or an AIM Implementation with a functionally equivalent Implementation. MPAI also defines 3 Interoperability Levels of an AIW executed in an AIF:

*Level 1 –* Implementer-specific and satisfying the MPAI-AIF Standard.

*Level 2 –* Specified by an MPAI Application Standard.

*Level 3 –* Specified by an MPAI Application Standard and certified by a Performance Assessor.

MPAI offers Users access to the promised benefits of AI with a guarantee of increased transparency, trust and reliability as the Interoperability Level of an Implementation moves from 1 to 3. Additional information on Interoperability Levels is provided in Annex 3.

# AI Health Secure Platform

This introduces the overall architecture of the AI-Health (Figure 1) which comprises a set of different actors, specific distributed services and APIs that will be described in the following sections.

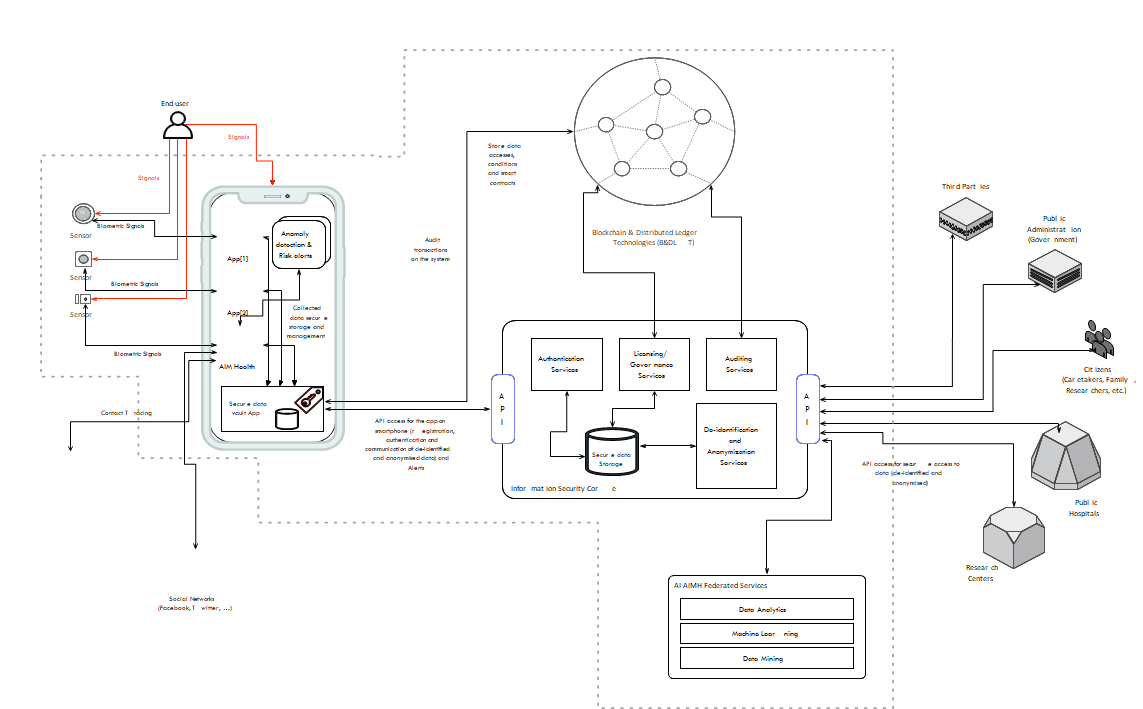


Figure 1 - Reference Model of MPAI-AIH Secure Platform

## Actors

The AI for Health data system identifies and recognizes the following different actors/entities.

* *End-user*: a user on the system for which their health-related data is going to be collected by the system. This end-user will control and audit the access of any third party to their health-related data according to the terms of a smart contract.
* *Third-party*: any third-party entity requiring access to the data on the system to process data and extract knowledge through the usage of some artificial intelligence mechanism (or through the orchestration of multiple intelligence mechanisms). This includes hospitals, clinics, research centers, caretakers, and others. Access is granted according to the terms of the smart contract between such a third party and the end-user. TBD: how the terms are verified for legal compliance
* *Medical data sources and Social Networks*: represent platforms from which the system may collect subsidiary data to make better symptoms prediction.

## Services

The AI for Health data system is composed by a set of distributed group components and services that are depicted in Figure 1. These group components are:

* The front-end system, a smartphone application that is capable of capturing, storing, and processing health-related data from the end-user. This data can be collected directly by some applications installed on the smartphone, such as Google Fit and Apple Health. Also, the smartphone will act as communication gateway to any external biometric sensors that also capture the health-related data events from the user. All the collected data will be securely stored on the user’s smartphone in a “Secure Data Vault” – access to this data vault is controlled by the end-user. The smartphone will also alert the end-user about any symptom that they could have derived from data processing.
* The back-end system, that is composed by a set of microservices that implement the necessary services to securely store data, to de-identify and anonymize data, to control entities authentication and access control to data, and to license and audit the access to health-related user data on the backend system. This system will gather anonymizes data from all the different sources (users and other possible sources) and will act has a broker gateway between the entities that would like to access data and those who will supply that data.

The system will also take advantage of Blockchain and Distributed Ledger Technologies (B&DLT). The objective of this B&DLT system is to enable the transparency and auditability of the system. Every health-related data access request will require the production of a license (smart contract) that will be stored on the B&DLT. This smart contract will contain information about the requesting entities (someone requesting access to data), the data requested, the access conditions (e.g., timeframe and the user permission). This information can be audited by the system and by the user to be sure that the data is being used according to what was established on the smart contract. TBD implications of the legal verification of the smart contract.

Finally, the system will also contain a set of AI services that can be used to process the data on the system to extract some specific knowledge. These services may be selected from different available ones and may be orchestrated to produce specific analyses for the entities that request access to health-related data. AI services may process the data and create machine learning models to identify and assist in the identification of diagnosis and prognosis.

## APIs

The system will use REST API interfaces that will provide data access by the end-user’s smartphone or a third-party external entity and the system backend. Another API will be implemented to create the interface between the system data and the AI modules that will use and process data. Data may also be collected from other sources such as public services and third-party entities, using specialized APIs.

# Healthcare use case

This section presents a simple use case[[2]](#footnote-2) that describes the system and its usage (Figure 2).

## User health data collection

1. The user signs into the system, which is equipped with the necessary security features and initializes the end-user secure data vault.
2. The user configures the smartphone app to connect to the different data sources (either external sensors or internal installed apps).
3. The MPAI-AIH app starts collecting data from the user and securely stores it locally on the smartphone.
4. The user is requested for permission to contribute their health data to the system. The user analyses the request and gives permission to contribute data (it may be all the data, or just some specific data). If the user gives access to their data, data will be collected on the system back-end.
5. The data from all the users participating in the system is collected by the global secure data storage where it will be de-identified and anonymized.

## Access to healthcare data

1. Any third-party entity may request data access. This entity needs to be properly registered and authenticated
2. The entity requests access to the data catalogue existing on the system, optionally selects the intelligent mechanisms that exist to process the data and extract some type of results and intelligence from the data.
3. This involves the selection of the specific tools to process the data (one tool, or multiple tools properly orchestrated) that can access the system data and perform some work with it. The existing tools to process data will be selected and instantiated to do the processing.
4. The entity accepts a smart contract created by the B&DLT on behalf of the end-user or a group of end-users. Access to data is permitted as long as the smart contract is valid.

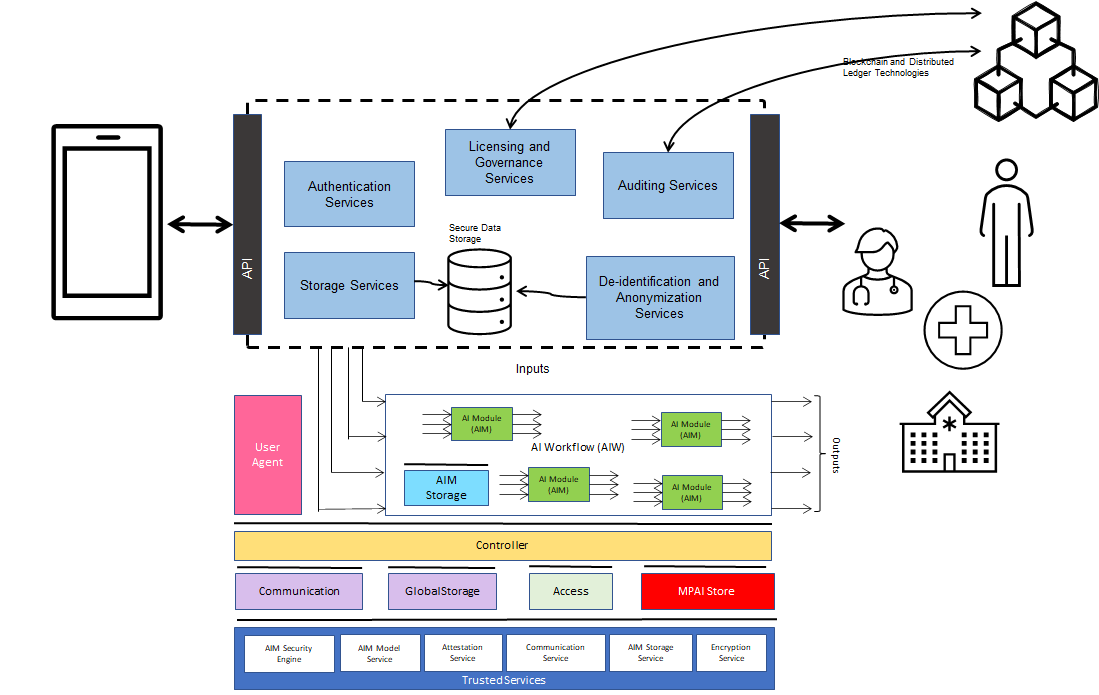


Figure 2 - AI-Health Federated Service

# Federated Services

## Federated Learning Mobile applications

(TBD rewording with a definition of FL) Federated learning can be used to build AI models on user’s health information from a data pool of smartphones without leaking personal data. For example, Google uses federated learning to improve on-device machine learning models like “Hey Google” in Google Assistant which allows users to issue voice commands.

## Healthcare Application Use Case

Healthcare and health insurance industry can leverage federated learning because it allows protection of sensitive data in the original source.

Federated learning models can provide better data diversity by gathering data from various locations (e.g., hospitals, electronic health record databases) to diagnose rare diseases.

The article [1] indicates that federated learning can help to solve challenges about data privacy and data governance by enabling machine learning models from non-co-located data.

## Federated Learning Processes

Two processes: training and inference.

### Training process

1. *Local machine learning (ML) models* are trained on local heterogeneous datasets. For example, as end-users use a machine learning application in their smartphones, they spot and correct discrepancies in the predictions of the machine learning application. These create local training datasets in each users’ device. Similarly, a user’s specific health data may be collected locally on the device and used to update a local model.
2. *The parameters of the models* are exchanged between smartphones, and smartphones and the backends system periodically. These parameters may be encrypted before exchanging. The fact that local data samples are not shared improves data protection and cybersecurity.
3. *A shared global model* is built as a result of the federated learning in a distributed fashion or by the backend system.

### Inference Process

The model is stored on the user device so predictions are quickly prepared using the model on the user device.

## MPAI-AIH Federated Components

End-user devices and third-party entities communicate with the MPAI-AIH Secure Platform using secure APIs, to provide and request data.

The AIWs at the bottom of Figure 2 can perform several operations, including the training and inference processes. The “MPAI Store” provides the AIWs and their AIMs.

This process is orchestrated by the controller which may use the different components (e.g., “communication”, “global store” and “access”) to communicate with the backend and perform desired operations.

Multiple instances of AIWs can exist and they can have the same or different objectives and can work with the same or different data, data sets or versions.

# References

1. Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H.R., Albarqouni, S., Bakas, S., Galtier, M.N., Landman, B.A., Maier-Hein, K. and Ourselin, S.; The future of digital health with federated learning; NPJ digital medicine, 3(1), pp.1-7; 2020.

1. ISCTE is funded by the Portuguese government to identify symptoms related to COVID-19, and heart and cardiac problems. [↑](#footnote-ref-1)
2. This should be considered as just a simple possible use case. Multiple usage scenarios may coexist in the system, but for simplicity purposes, we have just described a possible one. [↑](#footnote-ref-2)