ITUPublications

International Telecommunication Union
Standardization Sector

ITU-T Focus Group Deliverable

(03/2023)

Focus Group on Artificial Intelligence for Health (FG-AI4H)

FG-AI4H DEL5.5

Data handling

ITU-T FG-AI4H Deliverable DEL5.5

Data handling

Summary

ITU-T FG-AI4H Deliverable DEL5.5 outlines *how data will be handled*, once accepted. Health data is one of the most valuable and sensitive types of data. Handling this kind of data is often associated with a strict and factual framework defined by data protection laws. It is important to set a strict data policy which will ensure confidence in FG-AI4H, not only between contributors but across all stakeholders. There are two major issues that the data handling policy should address: a) compliance with regulations dealing with the use of personal health data; and b) non-disclosure of the *undisclosed test data* held by FG-AI4H for the purpose of model evaluation.

Keywords

Artificial intelligence, compliance, data handling, data protection, health, regulations, test data.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Change Log

This document contains Version 1 of the Deliverable DEL5.5 on "*Data handling*" approved on 16 March 2023 via the online approval process for the ITU-T Focus Group on AI for Health (FG-AI4H).

Editor: Marc Lecoultre
ML|LAB.AI
Switzerland
Email: ml@mllab.ai

Table of Contents

ITU-T FG-AI4H Deliverable DEL5.5

Data handling

1 Scope

Artificial Intelligence (AI) can help with achieving the important objective of ensuring health for everyone in many ways worldwide, often at reduced costs and enhanced speed. In the case of modern AI, it is important to notice that practitioners, patients and medical device regulators are confronted with a new kind of machine. While mechanical devices, electronics and software tools from the past have been typically designed from fully understood first principles, it is difficult to anticipate the behaviour of modern AI algorithms, because of the enormous complexity of the algorithms, and because the performance depends not only on the learning algorithm, but also on the underlying training data. These properties let the users raise doubts about whether they can trust AI models when they face critical decisions in the health domain. Crucially, these reasonable doubts cannot be resolved at present because there are no established ways to assess the quality of AI models for health.

The "Focus Group on Artificial Intelligence for Health" (FG-AI4H) will meet this need by demonstrating how the performance of AI solutions for health can be evaluated in a systematic fashion. For this purpose, a benchmarking framework will be developed in a best practice type of approach for representative use cases. Having successfully demonstrated the benefits of benchmarking for selected representative use cases, this will allow for expanding the approach to a wider range of use cases. Exemplary use cases may include AI-based diagnostics, treatment decision-making, triage, patient self-management, risk assessment, image segmentation or annotation and early detection, among others. Not all possible use cases can be addressed considering the limited timespan and resources of the focus group.

The core of the benchmarking framework consists of *undisclosed test datasets*, per use case of each topic area to be defined, that will not be made accessible to the AI developers. In addition, (a relatively small or large sets of) public data may be made available by FG-AI4H. We would like to note that data publication is not essential for the core idea of the benchmarking framework, but merely an optional extra, and that related problems have already been addressed by others before. Datasets are not limited to any modality such as images, time series, laboratory tests, "omics", text, or electronic health records, but a wide variety is welcome. Details of the envisioned benchmarking procedure are presented in the White Paper of FG-AI4H.

This document outlines how data will be handled once accepted, and states the governing principles and rules.

For sensible benchmarking, the topic drivers will address the following three dilemmas: 1) Benchmarking is not valid if AI techniques developed by data donors are tested on their own donated data because they know the data and associated output variables/labels. 2) Excluding data donors from benchmarking will considerably reduce the willingness to donate data, which is essential for a reasonable evaluation. 3) Having a data pool from several sources and testing each AI technique only on data from other sources (i.e., testing an AI technique developed by x only on data donated by y and z) may tempt data donors that also develop AI technology to contribute as "difficult" data (low quality data, wrong annotations, etc.) as possible to the data pool, in a competitive setting.

2 References

[FG-AI4H DEL07] ITU/WHO FG-AI4H Deliverable 7 (2023), *AI for health evaluation considerations.*

[ISO 7498-2] ISO 7498-2: 1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

[ISO 27001] ISO 27001: 2022, *Information security management systems – Requirements*.

[COM(2017)134] European Commission COM (2017) 134 final, *Communication from the Commission to the European Parliament, the Council, the European Economic And Social Committee and the Committee of the regions, European Interoperability Framework – Implementation Strategy*; Brussels.

3 Definitions

3.1 Terms defined in this Technical Report

This Technical Report defines the following terms:

3.1.1 public data: Subset of the *received data* that is made public by FG-AI4H to help AI developers to understand the structure of the undisclosed test data, or to train AI technology if enough data has been provided.

3.1.2 received data: Any dataset submitted by a sender and received by FG-AI4H.

3.1.3 undisclosed test data: Corresponds to the remaining *received data* after removing *public data*. This set is kept strictly private to evaluate submitted AI technology.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

AI	Artificial Intelligence
API	Application Programming Interface
CRUD	Create, Read, Update, Delete
EIF	European Interoperability Framework
EU	European Union
FG-AI4H	Focus Group on Artificial Intelligence for Health
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IPSec	Internet Protocol Security
IT	Information Technology
SSL	Secure Socket Layer
USB	Universal Serial Bus

5 Conventions

This Technical Report uses the following conventions:

– "Shall": states a **mandatory** requirement of this policy.

– "Should": states a **recommended** requirement of this policy.

– "May": states an **optional** requirement.

6 Data handling

Understanding the importance of data to our initiative and how that information is handled reflects our commitment as a secure organization. The purpose of a data handling policy is to ensure that all

sensitive data is confidentially controlled, whether it is being transmitted within the organization or to a trusted third party.

When handling data all users should be in accordance with, and be responsible for, adherence to strict rules to be defined in a reference document. Periodic auditing of adherence to this policy shall be the responsibility of FG-AI4H.

Data should be handled in the context of a multi-tiered security system that safeguards patient data according to government statute and regulations. Data should be hosted in secured data centres.

The system shall comply with all applicable regulations over the targeted countries (EU regulations, GDPR, US HIPAA, individual countries' healthcare privacy regulations, etc.). Regulations include information security, privacy and quality laws, guidelines and standards. We should design a regulatory compliance framework to ensure conformance with these regulations.

6.1 Legal context

There are a number of national and regional legislative initiatives aimed at defining horizontal frameworks for the protection of personal data, as well as intellectual property and trade secret rights, and as well as sector-specific legal frameworks targeting health data and its use for secondary purposes, such as, scientific research, development and innovation activities for products or services and training, testing and evaluation of algorithms of AI systems (Regulation on GDPR, Regulation on EHDS in the EU). In addition, legislation dedicated to AI is in force or is being prepared (e.g., the EU AI Act). Where national or regional data protection laws mutually differ, it is important to cover the most restrictive provisions to allow the greatest number of entities to share their datasets. This includes permission to use or access data, data security, anonymization, pseudonymization, access control and many other matters discussed in this document or detailed in relevant legislation.

6.2 Data security

The infrastructure for data storage and processing should be based on state-of-the-art security policies, practices and located in a secure location. Information should be securely received, stored and transferred. The encrypted transmission of datasets and encryption at rest (data stored encrypted) are among many other requirements. Only well-established and approved by FG-AI4H transfer methods should be used.

Where possible, data transfers should be carried out using existing, protected and trusted networks (internal to FG-AI4H or over a virtual private network with dedicated IPSec and SSL-encrypted channels). However, there may be occasions where data will need to be transferred via other networks such as the Internet or any other open networks. On these occasions, the data files should be protected by encryption to prevent usage by unauthorised parties.

In the case of a physical data transfer, e.g., USB flash or hard disks, all data should be securely stored in an encrypted format using a method approved by FG-AI4H. Transfers of data in hard copy format should be protected, using means such as qualified secure couriers.

6.3 Data integrity

Data integrity should be enforced when the data travels from one component to another using checksum mechanisms that guarantee that the data has not been corrupted or modified. *Any data files transferred or generated should be digitally signed and the data integrity of the payload should be validated at the edge of the network prior to storing the data in the database. This would ensure validation of data integrity of all raw and interpreted patient data.*

Any corrupt data (inaccurate or incomplete) should either be rejected by the system or removed from it.

The security and privacy architecture should be designed to ensure a high level of data integrity and privacy for protected health information in compliance with GDPR, US HIPAA, or any other participating country healthcare privacy, security, data access and quality regulations. This may be dependent on where the data was transferred from, where the data will be processed and by which entity.

6.4 Access control

Authorised stakeholders need to access the data for their own defined purpose and infrastructure administrators for maintenance. The receiving parties such as the working groups should evaluate and work on the datasets. The organizations that are willing to submit their algorithms need to access *public data* to develop their models. To guarantee absolute fairness among submitting organizations and ensure the credibility of the focus group, the *undisclosed test data* should remain undisclosed.

Clear access control should be defined and a database with detailed access rights policies should be implemented.

The system should authenticate users before any access to the system and its resources. The system should support standard authentication technique that can verify the identity claimed by the user (claims based, federated authentication, etc.).

Everyone willing to submit an algorithm should have access to the *public data*. The only restriction might be for the party submitting the *undisclosed test data*.

6.5 Auditing / logging

All transactions should be authenticated, authorized, monitored, and logged and audited regularly to detect unauthorized events. The system should detect events that can affect the confidentiality of personal health data or content of the *undisclosed test data*. The system should also record a trail of all processing of personal health information or *undisclosed test data*, such as viewing, creation, modification, validation, printing, copying, import, export, transmission and reception.

Unauthorized access attempts should be denied, and all requests should be logged and retained for audit purposes. Audit logs should be stored in encrypted form and decrypted only by recorded authorized requests and analysed as potential breaches.

6.6 Data lifecycle

The data lifecycle reflects all the steps and the related data processing and management capabilities followed by data from its creation to its use and disposal, and the way that it is created, read, updated, deleted and searched. This lifecycle is called the CRUD cycle. From a data point of view, the listed capabilities might affect the state and structure of data, the location of the data, its combination with other data, its transformation, its use and its disposal.

Processing and managing data requires effective data governance. Data governance refers to the overall management and caretaking of data, from creation to deletion, covering usability, integrity and security. The data governance process should be defined to determine which data is retained or deleted. Data should be kept, so in the case of the creation of a new benchmark, models could be retested.

Once the data has been received, it should be stored in a temporary location until data quality validation (verification or detection of any data abnormalities, see [FG-AI4H DEL07] for perturbation measures, bias and fairness measures and summary statistics for quality data) is completed before transfer to the production environment.

When required, data should be securely erased in accordance with a data destruction policy.

6.7 Data processing

Data processing is the ability to handle data as input and apply different treatments that might modify the data, or combine it without modifying it with other data in order to produce an output that is useful for a given application or service in the data lifecycle.

During the evaluation phase, *undisclosed test data* needs to be decrypted. We should ensure non-disclosure of the data during this critical phase.

6.8 Data ownership

The use and ownership of *received data* should be clearly defined in a licence agreement between the party providing the data (the owner of the data) and FG-AI4H.

6.9 Backup and archiving

Backed-up and archived data should have at least the same level of protection as production data, it should be encrypted. Both the backup and the archive should be located in a separate secure location, which is separate from the production data.

6.10 Interoperability

In case we foresee any need for interoperability with other health institutions and their information systems or participation in any open data initiatives, we might have to decide on a data hub/registry structure and selection of suitable standards.

Four layers of interoperability can be distinguished in Information Technology (IT) (e.g., European Interoperability Framework (EIF) is part of [COM(2017)134]):

– legal (laws adopted to allow these IT systems to cooperate with each other);
– organisational (organisations involved in the process should cooperate);
– technical (common standards, data exchange protocols shall be defined so that the AI-based IT solutions can interwork);
– semantics (all the participating systems shall use the same words/phrases and syntax to describe an object or a data request).

APIs/web services may be needed to enable different channels of data exchange to work with other systems and partners.

6.11 Compliance with international standards

Yearly audits should be conducted by internationally accredited auditors to confirm ITU/WHO observe obligatory security, data protection, continuity and compliance guidelines and procedures. This could comply with international standards such as [ISO 27001].

The security architecture for the data repositories should comply with security policies and privacy policies. The security solutions should be in alignment with the [ISO 7498-2] security model best practice recommendations on information security management.

6.12 Risk assessment

There should be periodic assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronically protected information held in the repository.

We should conduct a proactive periodic risk analysis of the audit logs and should take corrective action when unacceptable risks are identified. Proactive security measures sufficient to reduce risks and vulnerabilities to the level required by the data's high sensitivity shall be maintained throughout the programme's lifecycle.