|  |  |  |
| --- | --- | --- |
| ITU Logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | FG-AI4H-A-029-R1 |
| **ITU-T Focus Group on AI for Health** |
| **Original: English** |
| **WG(s):** | N/A | Geneva, 26-27 September 2018 |
| **DOCUMENT** |
| **Source:** | Marc Lecoultre |
| **Title:** | Brainstorming - Data handling policy |
| **Purpose:** | Discussion |
| **Contact:** | Marc LecoultreMLLab.aiSwitzerland | Tel: +41 79 321 09 29Fax: +41 22 364 30 69Email: ml@mllab.ai |

|  |  |
| --- | --- |
| **Abstract:** | This document is an initial draft and work in progress developed from initial discussions at the first FG-AI4H meeting, and it is planned to be be refined at the next FG meeting. This document proposes a preliminary outline of the data handling policy. Health data is one of the most valuable and sensitive data. Handling this kind of data is often associated with a strict and factual framework defined by data protection laws but may also involve emotional aspects; it is about biometric data that defines each of us, who we are, and what we have lived. It is important to set a strict data policy which will ensure confidence in FG-AI4H not only among contributors, but across all members of society.There are two major issues that the data handling policy should address:a) compliance with regulations dealing with the use of personal health data, andb) non-disclosure of the test datasets held by FG-AI4H for the purpose of algorithm evaluation. |

1. Definitions

In this document, we refer to different types of datasets. To clarify, we suggest the following definitions, taken from document [FGAI4H-A-006](https://extranet.itu.int/sites/itu-t/focusgroups/ai4h/_layouts/15/WopiFrame.aspx?sourcedoc=%7b6E723060-6525-4AD8-967C-DEAFFED9A3A6%7d&file=FGAI4H-A-006.docx&action=default)

Received data: Any dataset sent by a trusted source (tbd) and received by FG-AI4H;

Public data: Subset of the *Received data* that is made available by FG-AI4H to enable submitting organizations to train their models;

Test data: Two possibilities: 1) Corresponds to the remaining of the *Received data* after removing *Public data.* In a simpler way, it is *Received data - Public data*. 2) This set could be submitted by a different trusted source.This set is kept strictly private to evaluate submitted algorithms.

**2. Introduction**

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 sensitively data is properly handled whether being transmitted within the organization or to a trusted third party.

When handling data, all users shall do so in accordance with and be responsible for adherence to the Data Handling Policy. Periodic auditing of adherence to this policy shall be the responsibility of one Information Governance Team.

3. Legal context

In an international context, where national data protection laws may differ drastically, it is important to cover the most restrictive items to allow the greatest number of entities to share their datasets. This includes data security, anonymization, access control and many other discussed in this document.

For example, according to Art. 3 lit. c of the Swiss Federal Act on Data Protection (FADP), sensitive data are data on religious, ideological, political or trade union-related views or activities, health, the intimate sphere or the racial origin, social security measures, administrative or criminal proceedings and sanctions. These are subject to special protection and may, as a matter of principle, only be processed or forwarded for the purpose of external data processing with the consent of the subject. Such regulations might discourage and even forbid data holders to share their existing data.

We need to take special care of data that relates to an identified or identifiable person since the storage and processing of this kind of data falls under most of existing data protection laws.

4. Anonymization

Even though the *Received data* might contain data that relates to an identified or identifiable person, the Public data and Test data must not. The Received data should then be processed with appropriate methods to anonymize or pseudo-anonymize (cf. Aggregation of datasets) the dataset.

5. Data security

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

Where possible, data transfers should be carried out, using existing, protected and trusted networks (internal to FG-AI4H or over VPN: Virtual Private Network). However, there may be occasions where data will need to be transferred via other networks such as Internet. On these occasions, the data files must be protected by encryption to prevent usage by unauthorised parties.

In case of a physical data transfer, e.g. USB or hard disks, all data should be stored in an encrypted format using an approved by FG-AI4H method. Transfers of data in hard copy format will need to be protected, using such methods as approved couriers.

6. Access control

Different stakeholders need to access the data for their own purpose. Infrastructure administrators for maintenance. The receiving parties such as the Working Groups need to evaluate and work on the datasets. The organizations that are willing to submit their algorithms need to access the *Public data* to train their models. To guarantee absolute fairness among submitting organizations and ensure the credibility of the Focus Group, the test dataset (undisclosed) must remain undisclosed.

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

Should any organization willing to submit an algorithm have access to the Public data?

7. Data processing

During processing phase, data needs to be decrypted. In our case, this should not be a legal issue since the *Public data* only contains anonymized data. This is also the case for *Test data*. The focus needs to be on the processing of the *Test data* for the validation task to ensure non-disclosure of this data.

8. Data lifecycle

When dealing with data we need a good data governance. Data governance refers to the overall management and caretaking of data, from its creation to its deletion, covering usability integrity and security. Data governance will decide what data to keep or delete. Data could be kept until the creation of a new benchmark, in order to ensure models can be retested.

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

9. Compliance with international standards

Yearly audits should be conducted by internationally accredited auditors to check whether ICT/WHO observe applicable security, data protection, continuity and compliance guidelines and procedures. This could be done on the bases of international standards such as ISO 27001.

10. Data ownership

Data has become the new fuel of today’s world. To protect this valuable resource, the Focus Groups needs to guarantee ownership rights to the holders of data.

This involves questions like:

• Will data holders have to give up their rights or are they lending their data?

• Over which time period would data holders lend their data?

These issues are linked to point 4 (access control) of this document. Data ownership could be resolved using blockchain technology.

11. Aggregation of datasets

It would be valuable to have pseudo anonymization of data, i.e. no data relating to identified or identifiable person, but potential cross-references among different datasets. In the future, we will have enough datasets such that several data records will concern the same patient. If we could link these records together this would allow to constitute a broader (more biomarkers) or deeper (same measures over time) view of a single patient.

This approach could help discover new ways of making predictions by using different features than the pre-determined or pre-supposed ones. Here the term feature is referring to its use in the field of machine learning and corresponds to an individual measurable property or characteristic of a phenomenon being observed. For instance, to detect Glaucoma, the literature says that we need these features: age, ocular pressure, cornea thickness, visual field and retinal nerve fiber layer thickness values to make a good prediction.

Instead of limiting ourselves to this pre-established list, other/new factors should be considered.

We need to give us the chance to discover what we are not looking for. Science has often made big progress that way.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_