Accelerating the lab to market transition of AI tools for cancer management

CHAIMELEON Repository

Conditions of Use

Accessing to the CHAIMELEON Repository means that you accept the following terms and conditions of use.

Table of content

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 952172.

Accessing the CHAIMELEON Repository means that you are a Data User

If you provide a service by virtue of an employment relationship in a public or private legal person, your organisation is considered as the data user. If your access purpose is providing a service to third parties, you are responsible for complying with these terms and conditions.

In such a case, it is assumed that legal representative or a natural person who has been delegated the power of attorney for such acceptance has requested the access and the acceptance of the terms and conditions of use of CHAIMELEON Repository.

During your work in our information system, you must individually guarantee that you are aware of and accept our forbidden activities and mandatory security measures:

A. Forbidden activities:

The following purposes or processing activities are prohibited:

(a) taking decisions detrimental to a natural person based on their electronic health data; in order to qualify as “decisions”, they must produce legal effects or similarly significantly affect those natural persons;

(b) taking decisions in relation to a natural person or groups of natural persons to exclude them from the benefit of an insurance contract or to modify their contributions and insurance premiums;

(c) advertising or marketing activities towards health professionals, organisations in health or natural persons;

(d) providing access to, or otherwise making available, the electronic health data to third parties not mentioned in the data permit;

(e) developing products or services that may harm individuals and societies at large, including, but not limited to illicit drugs, alcoholic beverages, tobacco products, or goods or services which are designed or modified in such a way that they contravene public order or morality;

(f) re-identify the data;

(g) using the data for purposes other than those stated in the request;

(h) any act of misappropriation of the data, including the copying of the data on own premises, consultation by unauthorised persons or any conduct in breach of the conditions granted for access to the data;

(i) failure to comply with obligations under these terms and conditions and any specific conditions to which a particular access authorisation may be subject;

(j) any conduct contrary to the law, fundamental rights or public order that according to the applicable legal framework is prohibited and/or constitutes an administrative infringement or a criminal offence.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 952172.

B. Obligations

The authorised Data User shall:

(a) use the Data on the terms and for the purposes expressly authorized;

(b) Privacy-related obligations.

(c) comply with security measures;

1. Privacy-related obligations

User will take the following steps in order to protect the privacy rights of all individuals whose images are included within the Dataset:

a. User will not use the Dataset, either alone or in concert with any other information, to make any effort to identify or contact individuals who are or may be the sources of the information in the Dataset without specific written approval from the Responsible of the Repository. If User inadvertently receives identifiable information or otherwise identifies a subject, User will promptly notify Responsible of the Repository and follow Responsible of the Repository's reasonable written instructions.

b. User is strictly prohibited from generating or using images or comparable representations of the face, head, or body for facial recognition, reidentification, or other purposes that could allow the identities of research participants to be readily ascertained.

c. User will not request, and Responsible of the Repository will not release, the key codes to the Dataset to the User. Further, User will not request the key codes from any third parties that provided the Dataset to Responsible of the Repository.

d. User will follow relevant institutional policies and applicable European and national laws and regulations (if any) concerning the completion of ethics review or approval that may be required for the Project.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 952172.

2. Security obligations (including confidentiality and data breach procedure)

The CHAIMELEON Repository has appropriate security measures in place. As a user of an information system, you must comply with all security obligations that have been expressly notified to you and in particular:

- You accept that any of your activities in the Repository including your access is traceable. In this way, **your activity will be logged**.
- Both, with regard to ensuring the security of the Repository and the implementation of security measures to prevent unauthorised access to the Repository, you agree to maintain confidentiality and to ensure the security of the data, obligations that shall continue to apply even after the termination of your relationship with the use of the CHAIMELEON Repository.
- All the information is considered confidential.
- The media or equipment that you will use is managed by your organisation and it is a task of your organisation/company the guarantee of adequate security of such equipment.
- No data shall be collected or stored outside of the CHAIMELEON Repository.
- The equipment used to access the CHAIMELEON Repository will implement physical and logical access controls including measures like:
    - Password for computer use, which must not be stored in readable files, macros, or any other place where they can be accessed by unauthorised people.
    - In the case of user absence from the working place, the workstation/laptop must be locked, which must in any case occur automatically after 15 minutes of inactivity.
    - The screen computer position shall ensure that showed information is not accessible or legible to unauthorised people.
    - The computer shall be switched off at the end of the working period and shall not be used by unauthorised people.
    - Computer media containing protected information (like access credentials or just temporal information or pictures saved in cache) may not be donated to any third party without first having been completely and securely erased.
    - The user is responsible for Internet access that may compromise the security of its equipment.
    - Users must keep the operating systems, antivirus and firewalls of their work equipment updated.

- **Any security breach must be communicated urgently** to:
    - Breaches just related to security
        - security.chaimeleon-eu@i3m.upv.es
    - Security breaches that could involve privacy data
        - dpdchaimeleon@irtic.uv.es
    - Specifically when this involves:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 952172.

- A possible CHAIMELEON Repository access credential stolen or lost.
- A laptop with saved credential access stolen or lost.
- Any incident that, in the user opinion, could put the Repository at risk.

Responsibility

Violations of the obligations of these obligations or the legal framework generate liability and/or responsibilities. The Responsible of CHAIMELEON Repository may notify the authorities of such violations when it has a legal duty to do so.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 952172.