EUCAIM
CANCER IMAGE EUROPE

Project title: European Federation for Cancer Images
Project acronym: EUCAIM
Grant Agreement: 101100633
Call identifier: DIGITAL-2022-CLOUD-AI-02

EUCAIM's Legal Handbook for Data Protection Officers and Legal teams

Partner(s): UV
Author(s): Ricard Martínez Martínez
Date of delivery: 08/09/2025
Version: 1.0

Table of contents

1. Introduction

1.1 Purpose of the Legal Handbook

This Legal Handbook provides guidance to **Health Data Holders and Health Data Users** on the process of sharing or transferring data to the EUCAIM infrastructure. It details the legal and technical requirements for enrolling in the EUCAIM Federation. The handbook is specifically designed for Data Protection Officers (DPOs) of Data Holders, helping them understand and comply with the legal obligations required to establish a relationship with the EUCAIM Federation.

The sharing of data within the European Union is subject to a complex and evolving legal framework, which is still in the process of development and implementation. Ensuring robust ethical and legal guarantees—according to the ELSI Framework—is a demanding and specialized responsibility, especially in the context of sharing datasets, integrating nodes' data premises for federated data processing, reusing data, and developing, sharing or distributing software tools that interact with health data.

Organizations must also address strict cybersecurity obligations and may be required to comply with additional rules in regulated fields such as artificial intelligence, medical devices, or intellectual property. These requirements are particularly relevant when health data is shared for secondary use, repurposed for research or innovation, or when software is developed or made available within federated infrastructures like EUCAIM.

Providing accurate information and evidence to EUCAIM is essential, and it is strongly recommended that these tasks are carried out by professionals with expertise in the respective areas within each organization.

For a proper management of on boarding processes in any of the intended roles, three relevant aspects must be taken into account:

- **This Legal Handbook may not contain all requirements needed** (please check the rest of documentation); it is a legal explanation of the purposes for the legal and ethical requirements.
- From a legal perspective, the process requires the submission of self-declarations—typically by DPOs—and, whenever possible, supporting documentary evidence. However, **for the integration processes within EUCAIM, the provision of regulatory safeguards required by law, such as a Data Protection Impact Assessment (DPIA) or formal ethical approval, will be mandatory**. **Material verification will also apply to aspects like duly performed anonymisation, interoperability, and cybersecurity.** Failure to provide the necessary documentation for our due diligence and accountability, or failure to pass the implemented controls, authorizes EUCAIM to delay, suspend, or revoke any authorization or permission previously granted.
- A set of legal agreements must be signed and provided to state the obligations and responsibilities of the parties involved. The documents required are the evidence in order to join EUCAIM. The legal and ethical documents provided must ensure compliance with GDPR and/or any national laws.

1.2 Health Data Holders

Data holders are defined by EHDSR as:

> ‘health data holder’ means any natural or legal person, public authority, agency or other body in the healthcare or the care sectors, including reimbursement services where necessary, as well as any natural or legal person developing products or services intended for the health, healthcare or care sectors, developing or manufacturing wellness applications, performing research in relation to the healthcare or care sectors or acting as a mortality registry, as well as any Union institution, body, office or agency, that has either:
>
> (i) the right or obligation, in accordance with applicable Union or national law and in its capacity as a controller or joint controller, to process personal electronic health data for the provision of healthcare or care or for the purposes of public health, reimbursement, research, innovation, policymaking, official statistics or patient safety or for regulatory purposes; or
>
> (ii) the ability to make available non-personal electronic health data through the control of the technical design of a product and related services, including by registering, providing, restricting access to or exchanging such data;

Health Data Holders in EUCAIM are organizations that contribute with imaging and clinical datasets to the federated infrastructure (hereafter ‘the Platform’).

Among their responsibilities are ensuring compliance with legal, ethical and technical requirements, conducting proper anonymization and privacy risk assessments, and maintaining documentation and evidence of data provenance, ethical approval and GDPR compliance.

The following legal requirements are the evidence to corroborate the fulfilment of the mentioned duties.

1.3 Health Data Users

Health Data Users are defined by EHDSR:

> (u) ‘health data user’ means a natural or legal person, including Union institutions, bodies, offices or agencies, which has been granted lawful access to electronic health data for secondary use pursuant to a data permit, a health data request approval or an access approval by an authorised participant in HealthData@EU;

Health Data Users in EUCAIM are entities that usually will develop different processing activities such as data analytics or training Artificial Intelligence (AI) tools within the Platform.

Within the scope of Health Data Users, EUCAIM also includes applicants seeking access for the purpose of developing software or AI tools. This encompasses individuals or organizations who intend to leverage the platform's datasets and resources to build, validate, or perform proof-of-concept activities related to AI-driven healthcare solutions. These applicants, whether affiliated with an institution or acting independently, are considered Health Data Users when their primary objective is to use the data for testing, development, or innovation in AI and software applications, provided all regulatory, ethical, and security requirements are met.

Among the responsibilities of Health Data Users are ensuring compliance with legal, ethical and technical requirements, and maintaining documentation and evidence of it.

EUCAIM assumes that researchers and other users requiring access to data act under the responsibility of the organizations that employ them, such as universities, research centres, and companies. Data applicants who seek access as natural persons and act solely under their own responsibility are not exempt from any applicable legal obligations and responsibilities. All data users are required to adhere to the full spectrum of regulatory, ethical, and security requirements, regardless of their employment status or institutional affiliation.

1.4 Software and AI tools providers

The concept of Software and AI Tools Providers refers to those entities or individuals who collaborate with EUCAIM by integrating applications that are already marketed in production. These applications must comply with all legal and technical requirements applicable for their commercialization and deployment. Beyond general obligations, these providers are also required to ensure strict adherence to specific legal frameworks, such as the General Data Protection Regulation (GDPR), AI Act and to respect intellectual property rights.

In addition to meeting all standard and specific requirements, Software and AI Tools Providers collaborating with EUCAIM may be subject to certain guarantees. These may include, but are not limited to, the signing of data processing agreements (commonly known as processors agreements) and the precise definition of procedures relating to the management of intellectual property rights, trade secrets, and the rights of data re-users. The integration or collaboration process with EUCAIM may thus require additional contractual and organizational safeguards to ensure full compliance with regulatory, ethical, and proprietary standards.

2. On boarding Process

2.1 Contact person

It is essential to provide a contact person of the entity' legal team to be in close communication if needed with the legal team of EUCAIM. A contact point will be assigned during the on boarding process.

2.2 Initial requirements and commitments.

EUCAIM defines two main ways of participating in relation with health data, as Health Data Holders and/or Health Data Users. However, there is another way of participating into the project with no supply or use of health data directly, but by contributing to the EUCAIM platform, as Software or AI tool provider.

2.2.1 Health data Holders.

EUCAIM (European Cancer Imaging Initiative) is designed as an optimal infrastructure for the sharing of electronic health data specifically related to cancer. The platform facilitates the exchange of datasets generated through any means or procedures permitted by European or national legislation, encompassing research projects and consortia, data produced by hospitals and healthcare systems, health data originating from applications, and even data altruism initiatives. EUCAIM makes it possible for diverse entities—such as research organizations, hospitals, health systems, and other stakeholders—to contribute and access cancer-related health data. This approach ensures that research and innovation benefit from a broad spectrum of data sources, while maintaining full compliance with regulatory

requirements. To accommodate these varied data-sharing practices, EUCAIM has established two scenarios, each governed by a distinct legal instrument, providing clear and robust frameworks for participation:

- **Health Data Holders transferring data to our repositories**. This scenario applies to Health Data Holders who wish to transfer their datasets to EUCAIM's centralized or federated nodes repositories. It is particularly beneficial for completed research projects or organizations that seek long-term preservation and availability of their datasets for future research purposes. The process involves signing a Data Transfer Agreement (DTA) and sharing information about the datasets, metadata catalogue, and software. Health Data Holders formalize their participation by signing a Data Transfer Agreement (DTA), which outlines the terms and conditions under which data will be shared, processed, protected, and accessed (see 2.3 below). The DTA ensures compliance with all relevant data protection, privacy, and security obligations. EUCAIM guides contributors through the necessary steps, including data de-identification, and provides support throughout the process.
- **Federated Health Data Holders**: For organizations that manage active data repositories and wish to maintain their datasets locally within a federated environment, EUCAIM offers the option to participate as Federated Health Data Holders. In this case, the collaboration is formalized through a Data Sharing Agreement (DSA). The DSA establishes the terms for federated participation, including data sharing, processing, and security requirements, while enabling organizations to retain control over their data infrastructure. Entities provide information about their research projects, metadata catalogues, software, and local computational and storage capabilities. This model empowers participants to contribute to EUCAIM while maintaining autonomy over their data assets.

Both the DTA and DSA are legally binding agreements that guarantee all parties understand and accept their obligations regarding data protection, privacy, and security. EUCAIM ensures that all shared health data is handled in accordance with the highest standards of European and national legislation, including GDPR and the European Health Data Space Regulation (EHDSR).

2.2.2 Health Data Users

- **Data access applicants.** Applicants seeking access to data must fully comply with the ethical and legal requirements established by the GDPR and the EUCAIM framework based on EHDSR. They are required to provide comprehensive legal and ethical documentation, which will be subject to verification by the EUCAIM Access Committee to ensure conformity with all applicable standards and safeguards. In the event that access is authorised, the legal representatives of the applicant entities must formally accept the EUCAIM terms and conditions. Furthermore, every individual user within each authorised entity is obliged to accept specific security obligations and must sign a binding commitment not to attempt the re-identification of data subjects.
- **Software and AI Systems developers:** in order to train or execute an Artificial Intelligence (AI) tool within the EUCAIM project, organisations will need to demonstrate with evidence that the AI tool/system comply with GDPR (if needed), AI ethics and the European Health Data Space Regulation. In such cases, it may be

required to demonstrate compliance with appropriate ethical standards and to provide evidence that ensures the robustness of the application and that it poses no risk to the security of EUCAIM. No AI tool/system without appropriate and robust security will be implemented in the EUCAIM platform.

2.2.3 Software and AI tools providers

To guarantee a reliable and secure processing environment for all participants, EUCAIM requires that any AI tool or system intended for training or deployment on the platform demonstrates full compliance with all applicable legal and ethical standards. We are referring to software or systems based on artificial intelligence that are integrated both into the application dashboard and the pool of tools available for orchestrating and analysing data within the EUCAIM platform. Evidence of robust security measures and risk mitigation must be provided. Only AI tools and systems that meet these stringent requirements will be allowed for integration within the EUCAIM infrastructure.

2.3 Health Data Holder's on boarding Workflow

The on boarding workflow for Health Data Holders includes an initial assessment for retrieving all information through the Tier's Maturity Level Questionnaire, which will allow EUCAIM Federation to assess that Data Holders' datasets act in accordance with any national and European legislation.

If a Health Data Holder, such as a hospital, wishes to join within a federated data processing framework, it is essential to complete the Data Warehouse Maturity Questionnaire to demonstrate the maturity of the organization's data storage and processing environments.

Afterward, the Health Data Holders will select the integration method (Reference Node or local Federated Node) and provide the compliance documentation shown in the different documents available for this process.

2.3.1 Requirements for Health Data Holders.

2.3.1.1 Contact person

To facilitate a smooth and effective on boarding process, it is strongly recommended that each Health Data Holder appoint a contact person from their legal team who will serve as the primary liaison with the EUCAIM legal team. Establishing this direct communication channel not only expedites responses to compliance queries and legal clarifications but also increases overall efficiency, reducing delays related to documentation and approval.

It is also particularly advantageous for this designated contact person to possess a thorough understanding of the EUCAIM Project and its procedures. Familiarity with EUCAIM's requirements and operational framework enables proactive engagement, helps anticipate potential challenges, and fosters a collaborative atmosphere in which regulatory obligations are met seamlessly. This approach ensures that both the Health Data Holder and EUCAIM can rapidly address any legal or ethical matters, streamline the integration workflow, and maintain the highest standards of accountability and transparency throughout the partnership.

2.3.1.2 Required documents

▪ **General Statements**

(a) Document identifying the legal representative and certifying their explicit authority to sign agreements and enter into binding commitments on behalf of the entity.

It should be noted that this identification is required solely for the engagement procedure. In all cases, formal legal evidence of the power of attorney must be presented either at this step or prior to the signature of any data sharing or transfer agreements, or the undertaking of any other binding commitments.

(b). DPO statement that confirms the awareness and the lawfulness of the adhesion to EUCAIM scheme.

This statement establishes foundational expectations regarding data protection, legal compliance, and ethical responsibility. Its purpose is to ensure that the participant uphold a consistent standard of trustworthiness, accountability, and security, thereby fostering a reliable and ethically sound environment. In addition, this statement may include the identification of the legal representative, explicitly confirming their authority to sign agreements and make binding commitments on behalf of the organization.

▪ **Relevant supporting documents or reports may also be attached as part of the submission.**

For the purposes of the onboarding process, it is acceptable to submit a responsive declaration from the Data Protection Officer (DPO) addressing these issues. However, the subsequent requirement regarding the provision of formal legal evidence remains strictly compulsory and cannot be waived. This ensures that while initial compliance and awareness can be promptly validated, all binding commitments and agreements will only proceed upon receipt of the necessary formal documentation.

(a) GDPR compliance may be documented by:

- DPIA (if required)
- Risk analysis report or audits by third parties.
- Adherence to codes of conduct or certification schemes.
- DPO report/self-declaration on GDPR compliance (a template will be provided).

(b) Security Compliance may be documented by:

- ISO 27001 security certification or any other national framework (such as Spanish National Security Framework - ENS) or adherence to official code of conduct recognised by EDPB (only if the applicant indicated Tier 3 compliance)
- An audit report issued by an independent officer or third party, attesting to the effectiveness of implemented measures or a report of the Chief Information Security Officer (CISO).

(c) Evidence of the adequate anonymization/pseudonymisation process that has been carried out.

(d) Any documents and other restrictions required under the data holder's national legislation

Restrictions on data reuse imposed by national law or by the conditions of the specific data set must be clearly documented. This includes, for example, any purposes explicitly prohibited by law, limitations arising from the scope of patient consent (such as data that may be used only for certain research areas), or records of individuals opting out of data

sharing or reuse. Evidence of these restrictions should be included with the submission to ensure that all data processing activities respect legal and ethical boundaries.

(e) Ethics requirements may be documented by:

- Ethical approval.
- Self-assessment/ethical report if applicable.
- Exemption statement by national law. If an ethical approval or self-assessment/ethical report is not needed in the establishment country, submit a DPO self-declaration. This information could also be incorporated into the DPO's report referenced in item 2.

2.3.1.3 Rationale for Requiring Supporting Documentation

It is essential to recognise that our activities unfold within a dynamic and multifaceted legal landscape, shaped by both current and emerging regulations. As data holders, we are bound to fully comply with the General Data Protection Regulation (GDPR), while simultaneously preparing for the anticipated alignment with the European Health Data Space Regulation (EHDSR) and the AI Act. Such legal changes demand proactive adaptation, rigorous oversight, and continuous review of our data stewardship practices.

Organizations must ensure full compliance with patient data protection rights as mandated by GDPR Article 9 and EHDSR provisions. All data processing activities shall maintain strict regulatory compliance. By prioritising ethical standards, data security, and robust anonymization measures, EUCAIM aims to build and maintain a foundation of confidence in our operations—ensuring that every data processing activity is conducted with the utmost respect for patient autonomy, privacy, and dignity.

A. Power of attorney

The designation of a legal representative is mandatory. The signing of any documentation that binds the entity with EUCAIM will be taken in the name and on behalf of the Health Data Holder by the legal representative. In the case of the data transfer or data sharing process involves multiple data holders (such as a research consortium or any other kind of cooperation agreements), proof of legal representation is also needed.

Legal representatives should verify that datasets, tools, or software are being shared in accordance with the law. This not only protects the EUCAIM project but also safeguards the participant entities from potential legal liabilities.

For the sake of procedural simplification, EUCAIM accepts that, during the initial engagement process, the notification regarding the identity of the legal representative may be included in the DPO statement. Power of attorney may be demonstrated by any document valid under the law of the applicant's country of establishment, such as:

- General or special power of attorney eventually notarized or registered.
- Statutory Representation.
- Mandate or agency contracts.
- A provision published in an official gazette.
- The documentation must prove that the legal representative is authorized to formalize the agreements required by EUCAIM.
- Any other legal valid instrument.

Please note: Principal Investigators (PIs) usually do not have legal authority to sign contracts on behalf of their institution. It is essential to verify who holds legal representation for such matters. If you are a PI, we recommend that you contact your institution's legal support services to confirm the appropriate representative.

B. General Data Protection Regulation compliance

Although EUCAIM's institutional design is focused on the processing of anonymized data, it remains imperative that the creation of any data set strictly adheres to the requirements of the GDPR. Failure to ensure such compliance may result in the generated dataset violating applicable data protection laws.

- Lawful origin of the data and lawful basis for processing:
  - Lawful Origin of the Data: Documentation must be provided to demonstrate the provenance of the data. This evidence should confirm that the data was collected in accordance with all relevant legal standards, ensuring its origin is legitimate and traceable.
  - Lawful Basis for Processing: Proof must also be supplied to establish the legality of processing activities, as outlined in Articles 6 and 9 of the GDPR and National Law. This includes showing that sharing or transferring the data is conducted on valid legal grounds. Where multiple data holders are involved, such as in a consortium or any other cooperation agreement, documentation confirming the lawful basis for each party's data processing is required.

Evidence provided by DPO report on Lawful origin of the data and lawful basis for processing. Where the DPO states the origin of the data, and the fact that it has been legally collected according to European and national law, it will be considered as a document demonstrating lawful origin of the data. The DPO report should provide clear documentation confirming both the lawful origin of the data and the legal grounds for processing it. If the DPO certifies that the data was collected in line with all European and national laws, this report can serve as proof that the data meets legal requirements for origin and processing.

- GDPR DPIA:

  The data holder must demonstrate compliance with GDPR, and any national law related to Data Protection, by providing a Data Protection Impact Assessment (DPIA) if needed:

  - Tier 1 and Tier 2 compliance

    If the organization is classified as Tier 1 or Tier 2, the Data Protection Officer (DPO) is responsible for determining whether a Data Protection Impact Assessment (DPIA) is necessary, following Article 35 of the GDPR, national laws, and the guidance provided by the national data protection authority regarding activities that require a DPIA.

    If the organisation is exempt from being required to submit a DPIA, it may be asked to provide risk assessments, independent audits, evidence of membership in codes of conduct or participation in certification schemes, or equivalent evidence

    However, if the organization does not have a DPO report confirming that a DPIA is unnecessary under Article 35 of the GDPR, national law, or the national data protection authority, EUCAIM will deem a DPIA to be mandatory.

  - Tier 3 compliance

If the maturity level is Tier 3, a DPIA is compulsory due to EUCAIM requirements. In this case, it is advisable to implement a DPIA. If a DPIA is not available, it will be mandatory to provide support to the EUCAIM staff for its preparation. If this collaboration does not take place, integration will not be possible.

C. GDPR and EHDSR requirements on security for health data holders or entities playing the role of federated nodes

Recital (77) of the EHDSR describes that all secondary use access to the requested electronic health data should be done in a secure processing environment, which according to Regulation (EU) 2022/868 is the physical or virtual environment to determine and supervise all data processing actions that ensures compliance with European Union law, such as Regulation (EU) 2016/679.

Health Data Holders that will play the role of federated nodes should guarantee security specifications that define their infrastructure in accordance with EHDSR. In addition to the conditions of Tier maturity level specified by EUCAIM, the minimum legal obligations of Article 73 of EHDSR states that the secure processing environment shall comply with the following security measures:

a) the restriction of access to the secure processing environment to authorised natural persons listed in the data permit issued pursuant to Article 68;

b) the minimisation of the risk of the unauthorised reading, copying, modification or removal of electronic health data hosted in the secure processing environment through state-of-the-art technical and organisational measures;

c) the limitation of the input of electronic health data and the inspection, modification or deletion of electronic health data hosted in the secure processing environment to a limited number of authorised identifiable individuals;

d) ensuring that health data users have access only to the electronic health data covered by their data permit, by means of individual and unique user identities and confidential access modes only;

e) the keeping of identifiable logs of access to and activities in the secure processing environment for the period necessary to verify and audit all processing operations in that environment; logs of access shall be kept for at least one year;

f) ensuring compliance and monitoring the security measures referred to in this paragraph to mitigate potential security threats.

This will be evidenced through documentation attesting to the security conditions established by the environment.

- ISO 27001 security certification or any other national framework (such as Spanish National Security Framework - ENS) or adherence to official code of conduct recognised by EDPB (only if the applicant indicated Tier 3 compliance).
- In the case there is no available an ISO 27001 security certification, an audit report issued by an independent officer or third party or a report of the Chief Information Security Officer (CISO) will be requested, and it will address:
  - Description of security measures taken;
  - Commitment to GDPR security measures;

- Confirmation that the applicant is able to meet EUCAIM requirements related to security;
- If applicable, reference to any internal or national standard followed by the candidate applicant.

D. Ethics requirements

- Ethical approval: Recital 73 of Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space (EDHS) indicates that an ethical assessment could be requested based on national law. In this case, the entity must provide a certificate of approval validly issued by an ethics committee.

  If it is not required by the national law, it will be needed a certification that demonstrates it is not requested, issued by a committee with the competence to do so, or a risk self-assessment.

  For health data and research, national requirements vary widely. Some countries require ethical approval for secondary data use, while others require risk assessments or an internal protocol to manage the risks detected. To ensure legal and ethical adherence, EUCAIM requires one of the following:

  - Formal ethical approval issued by a recognised committee;
  - Certification of exemption from such approval;
  - Or internal risk assessments and protocols.

  This ensures that any datasets or AI tools shared within the project meet both ethical and legal standards.

E. Additional documentary evidence

It is important to note that, under the General Data Protection Regulation (GDPR), particularly articles 9.2 and 9.4, significant authority is conferred upon Member States to establish national rules governing the processing of health data. This distribution of powers means that, beyond the overarching EU framework, national legislation can introduce specific requirements or limitations—especially in relation to the secondary use of health data.

In anticipation of ongoing developments and the future implementation of the EHDSR and related EU health data regulations, it is therefore essential that applicants provide comprehensive information regarding any national requisites that may apply. This includes, but is not limited to, additional documentary evidence or certifications required by national law, and detailed descriptions of any restrictions governing secondary data usage. Such transparency is vital to ensure that all legal and ethical conditions are met, and that the practices adopted by Health Data Holders and Users remain fully compliant with both EU and national legislation. The health data holder should provide:

- Any documents required under national legislation (e.g., authorization from a data protection authority, health authority, or any other relevant body): regarding the national legislation where the Data Holder is established in.
- Other restrictions that should be requested to data holder: in accordance Chapter IV “Secondary use” of European Health Data Space Regulation, the national Law of Member States may provide some conditions and restrictions on secondary use of data that may affect the Data Holders.

F. Agreements signature

Besides the requirements aforementioned, there are some essentials left depending on the different collaboration model chosen by the data holders.

- If Health Data Holders agree to transfer data to a **reference node**, the signed DTA with its annexes and the Terms and Conditions for the data are necessary. Terms of Usage means compliance with transparency, accountability and purpose limitations.
- In the event that Health Data Holders want to set up their own **federated node**, they will also furnish the signed DSA with its annexes, the Data Protection Impact Assessment (DPIA) congruent with article 35 of GDPR, as a guarantee that they can fulfil the security, and documents demonstrating the security of the information system, according with article 32 of GDPR.

2.3.3 Additional requirements for processing anonymized v. pseudonymised electronic health data

EUCAIM is based on the sharing of anonymized data. According to Opinion 05/2014 on Anonymization Techniques[1], data protection authorities require that any data intended for anonymization must be collected lawfully and for a clearly defined purpose. Since anonymized data is originally derived from personal data, its initial collection must comply with Articles 5, 6, and 9(2) of the GDPR.

Health data holders must provide duly anonymized datasets, reserving the infrastructure and the ability to try to establish the risk of re-identification. When Health Data Holders are willing to transfer or share anonymized data, they shall provide evidence of the conditions for anonymization of the data and confirm that adequate anonymization is ensured. Those health data holders who need support or assistance for a duly anonymization from the infrastructure or one of its partners, will be able to formalize the appropriate data processor contract that legally supports this provision.

If Health Data Holders are willing to transfer or share pseudonymised data, they shall provide evidence of the conditions related to the pseudonymisation of the data. If consent was needed when it is used as the legal basis of the processing according to article 6(1) (a) of GDPR), it must be able to demonstrate an appropriate consent that shows it meets the basic principles of processing personal data (article 5 of GDPR) and inform about the rights of the subject data (articles 12 to 23 of GDPR). In the case of processing pseudonymised data without the data subject's consent, it must be demonstrated whether exceptions to patient consent operate under national law.

It should be noted that EUCAIM has been specifically designed with a commitment to the processing of anonymized data. The sharing of pseudonymised data will require a case-by-case evaluation and must be expressly approved by the Consortium.

2.4 Data Users on boarding Workflow

2.4.1 Requirements for Health Data Users.

2.4.1.1 Contact person

To facilitate a smooth and effective on boarding process, each Health Data User shall appoint a contact person from their legal team who will serve as the primary liaison with the

[1] See https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

EUCAIM legal team. Establishing this direct communication channel not only expedites responses to compliance queries and legal clarifications but also increases overall efficiency, reducing delays related to documentation and approval.

It is also particularly advantageous for this designated contact person to possess a thorough understanding of the EUCAIM Project and its procedures. For this reason, it is strongly recommended that researchers interested in participating in EUCAIM and requesting access to data for reuse notify their legal support team from the earliest stages of the process. Providing them with this legal handbook, along with the call text and any other relevant documentation, will enable the legal team to offer effective assistance both in handling the EUCAIM procedures and in fulfilling the various ethical and regulatory requirements that may apply according to national and European regulations to his/her research activity and eventual data processing. This proactive collaboration not only streamlines the administrative process, but also strengthens legal certainty and ensures that every stage of the procedure is carried out under the highest standards of transparency and compliance.

Familiarity with the EUCAIM's requirements and operational framework enables proactive engagement, helps anticipate potential challenges, and fosters a collaborative atmosphere in which regulatory obligations are met seamlessly. This approach ensures that both the Health Data Holder and EUCAIM can rapidly address any legal or ethical matters, streamline the integration workflow, and maintain the highest standards of accountability and transparency throughout the partnership.

2.4.1.2 Required documents

- **General Statements**

a) Document identifying the legal representative and certifying their explicit authority to sign agreements and enter into binding commitments on behalf of the entity.

It should be noted that this identification is required solely for the engagement procedure. In all cases, formal legal evidence of the power of attorney must be presented either at this step or prior to the signature of any data sharing or transfer agreements, or the undertaking of any other binding commitments.

(b). DPO statement that confirms the awareness and the lawfulness of the adhesion to EUCAIM scheme.

The DPO Statement should formally confirm to EUCAIM that the supporting entity is fully aware of the data request. Furthermore, it must assure that all relevant staff—particularly researchers and data analysts—have received thorough training in key areas such as privacy, confidentiality, and AI literacy. This declaration serves to demonstrate that the team is equipped to meet both legal requirements and the compliance standards set forth by EUCAIM's best practices.

In addition, this statement may include the identification of the legal representative, explicitly confirming their authority to sign agreements and make binding commitments on behalf of the organization.

- **Relevant supporting documents or reports may also be attached as part of the submission.**

For the purposes of the on boarding process, it is acceptable to submit a responsive declaration from the Data Protection Officer (DPO) addressing these issues. However, the subsequent requirement regarding the provision of formal legal evidence remains strictly

compulsory and cannot be waived. This ensures that while initial compliance and awareness can be promptly validated, all binding commitments and agreements will only proceed upon receipt of the necessary formal documentation.

(a) GDPR compliance may be documented by:

- DPIA (if required)
- Risk analysis report.
- DPO report/self-declaration on GDPR compliance (a template will be provided).

It should be clarified that, as a general rule, EUCAIM provides an environment for the processing of anonymized data. Therefore, the GDPR does not apply. However, it would not be unusual for processing activities to require a DPIA in the following cases: when its completion has been committed to (a) either by virtue of the conditions of a grant or contract; (b) as a good practice or upon recommendation from the institution, the health system, or a supervisory authority; or (c) when the outcome obtained will be applied to individuals/patients in order to process personal data or generate new personal data. In such cases, support from EUCAIM may be requested for the implementation of the risk analysis or DPIA, and users may access information about the conditions of our secure processing environment and the legal safeguards we offer to data users.

(b) Security Compliance may be documented by:

Entities authorized to use EUCAIM must provide two kinds of guarantees to ensure compliance and responsible use of the data platform.

- Terms & Conditions. Firstly, each entity must accept the EUCAIM Terms and Conditions, formally recognizing their legal obligations within the framework defined by EUCAIM.
- Data users' commitments. Furthermore, every user authorized to access EUCAIM on behalf of the entity is required to subscribe to two distinct commitments, each expressing a differentiated set of obligations:
    - Acceptance of Security Obligations: Each user must agree to comply with the security requirements of the secure processing environment provided by EUCAIM. This means respecting all technical and organizational measures designed to protect the integrity, confidentiality, and lawful processing of data within the platform.
    - Commitment to Non-re-identification: Users must explicitly commit to refraining from any activity that could lead to the re-identification of data subjects. Under no circumstances may authorized users attempt to reverse anonymization or pseudonymisation processes, or otherwise seek to identify individuals from the data sets accessed through EUCAIM.

These obligations are essential to safeguarding privacy and ensuring that both entities and individual users act within the ethical and legal boundaries established by EUCAIM and applicable legislation.

(c) Ethics requirements may be documented by:

- Ethical approval.
- Self-assessment/ethical report if applicable.

- Exemption statement by national law. If an ethical approval or self-assessment/ethical report is not needed in the establishment country, submit a DPO self-declaration. This information could also be incorporated into the DPO's report referenced in item 2.
- AI impact assessments (ALTAI), and Fundamental Rights Impact Assessment (FRIA) if applicable. The use of AI within the EUCAIM framework should include acknowledgment of compliance with all relevant legal and ethical obligations, such as those set out by the AI Act and the necessary impact assessments (e.g., ALTAI, FRIA) where applicable.

2.4.1.3 Rationale for Requiring Supporting Documentation

It is essential to recognise that our activities unfold within a dynamic and multifaceted legal landscape, shaped by both current and emerging regulations. Organizations must comply with current GDPR requirements and prepare for EHDSR implementation. As data users, we are bound to fully comply with the General Data Protection Regulation (GDPR), while simultaneously preparing for the anticipated alignment with the European Health Data Space Regulation (EHDSR) and the AI Act. Such legal changes demand proactive adaptation, rigorous oversight, and continuous review of our data stewardship practices.

Above all, our guiding principle is an unwavering commitment to the rights of patients whose data we are entrusted to safeguard. Our dedication extends beyond mere legal compliance: we seek to foster certainty, reliability, and trust among stakeholders and the wider public across European societies. By prioritising ethical standards, data security, and robust anonymization measures, we aim to build and maintain a foundation of confidence in our operations—ensuring that every data processing activity is conducted with the utmost respect for patient autonomy, privacy, and dignity.

A. Power of attorney

The designation of a legal representative is mandatory. The signing of any documentation that binds the entity with EUCAIM will be taken in the name and on behalf of the Health Data User by the legal representative.

It is important to clarify that individual researchers or data users are generally not vested with the authority to enter into binding agreements or undertake legal obligations on behalf of their institutions. The power and responsibility to formalise such commitments reside with the employing entity, which holds both the legal capacity and the duty of care required by the EUCAIM framework. While EUCAIM recognises that initial data access applications may originate from individual researchers, the final authorisation and execution of any contractual or legal obligations must be undertaken by the entity itself, through its designated legal representative. This ensures that all institutional obligations are properly fulfilled, safeguards the interests of all parties, and upholds the integrity and compliance of the overall process.

For the sake of procedural simplification, EUCAIM accepts that, during the initial engagement process, the notification regarding the identity of the legal representative may be included in the DPO statement. Power of attorney may be demonstrated by any document valid under the law of the applicant's country of establishment, such as:

- General or special power of attorney eventually notarized or registered.
- Statutory Representation.

- Mandate or agency contracts.
- A provision published in an official gazette.
- The documentation must prove that the legal representative is authorized to formalize the agreements required by EUCAIM.
- Any other legal valid instrument.

Please note: Principal Investigators (PIs) usually do not have legal authority to sign contracts on behalf of their institution. It is essential to verify who holds legal representation for such matters. If you are a PI, we recommend that you contact your institution's legal support services to confirm the appropriate representative.

B. General Data Protection Regulation compliance

Although EUCAIM's institutional framework primarily centres on the processing of anonymized data, it is crucial to recognise the broader legal implications that may arise. Importantly, we must emphasise that obligations under the GDPR can still be triggered by the processing of data that is anonymized or considered non-personal, depending on the ultimate purposes of that processing.

C. EHDSR requirements

Within this evolving regulatory landscape, the EUCAIM initiative is designed explicitly to promote secondary uses of health data that are accepted under the European Health Data Space Regulation (EHDSR), while simultaneously establishing robust measures to prevent any uses that are forbidden under EHDSR and the Artificial Intelligence (AI) Act.

The EHDSR recognises the immense value of health data when used for purposes beyond primary clinical care—such as scientific research, innovation, development of new treatments and AI-driven healthcare solutions—provided such uses align with legal, ethical, and data protection standards. EUCAIM's policies therefore facilitate secondary uses which are permitted when data is processed lawfully, with adequate safeguards for privacy, and under the oversight of authorised entities.

Conversely, EUCAIM strictly prohibits any secondary uses that would contravene EHDSR or the AI Act. Forbidden uses include, for example, processing health data for discriminatory profiling, commercial exploitation without consent, or for purposes inconsistent with public interest or fundamental rights. Under the AI Act, the deployment of AI systems in healthcare is subject to additional bans and limitations—such as prohibitions on AI technologies that pose unacceptable risks (e.g., systems manipulating human behaviour or exploiting vulnerabilities of specific groups), or that lack transparency and accountability mechanisms.

In summary, EUCAIM's operational policy upholds the dual objective of fostering innovation and research through lawful secondary data use, while vigilantly guarding against any processing or AI application that would be deemed unlawful, unethical, or prohibited under current EU regulations.

E. Ethics requirements

- Ethical approval: Recital 73 of Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space (EDHS) indicates that an ethical assessment could be requested based on national law. In

this case, the entity must provide a certificate of approval validly issued by an ethics committee.

If it is not required by the national law, it will be needed a certification that demonstrates it is not requested, issued by a committee with the competence to do so, or a risk self-assessment.

For health data and research, national requirements vary widely. Some countries require ethical approval for secondary data use, while others require risk assessments or an internal protocol to manage the risks detected. To ensure legal and ethical adherence, EUCAIM requires one of the following:

- Formal ethical approval issued by a recognised committee;
- Certification of exemption from such approval;
- Or internal risk assessments and protocols.

This ensures that any datasets or AI tools shared within the project meet both ethical and legal standards.

- AI Ethics. In cases where the intended use may fall under research conditions established by the AI Act, it could be necessary to conduct ethical risk management according to the ALTAI principles, or to implement Fundamental Rights Impact Assessments (FRIA). These measures ensure that the deployment of AI systems in research not only aligns with legal mandates, but also proactively safeguards ethical standards and fundamental rights throughout the lifecycle of data processing and application.

E. Additional documentary evidence

It is important to note that, under the General Data Protection Regulation (GDPR), particularly articles 9.2 and 9.4, significant authority is conferred upon Member States to establish national rules governing the processing of health data. This distribution of powers means that, beyond the overarching EU framework, national legislation can introduce specific requirements or limitations—especially in relation to the secondary use of health data.

F. Agreements signature

Ensuring rigorous compliance and unwavering legal alignment with European Union laws is foundational to the EUCAIM project. In light of this, we must communicate clearly to the legal teams the existence and criticality of three mandatory agreements that every participating entity and authorised user must uphold. These agreements are not merely procedural; they are central pillars that support our commitment to robust governance, protection of patient rights, and the cultivation of trustworthiness within society at large.

- Terms and Conditions Agreement. The primary and most significant agreement is the formal acceptance of the Terms and Conditions by the participating entity itself. This ensures that the organisation acknowledges and commits to the legal, ethical, and operational standards required by EUCAIM, including compliance with GDPR, the AI Act, and relevant sector-specific regulations. Only after the entity has accepted these Terms and Conditions will individual users be authorised to access the platform and its resources. This agreement is the cornerstone of our compliance framework, setting expectations and responsibilities at the organisational level.
- Authorised User Security Obligation Agreement. Each authorised user with access to EUCAIM must explicitly accept their personal responsibility regarding data security.

This encompasses safeguarding sensitive health data and adhering to all prescribed security measures and protocols, as dictated by the platform and by law. This agreement also affirms the user's understanding of the potential risks involved and the necessary actions to mitigate them, reinforcing a culture of vigilance and accountability.

- Non-re-identification Commitment Agreement. Every authorised user must formally commit to the principle of non-re-identification. This means refraining from any attempt to reidentify individuals from anonymized or pseudonymised data, thereby upholding the privacy and dignity of patients whose information is processed within EUCAIM.

Our approach to compliance is not passive; it is robust and proactive. By requiring both organisational and individual commitments, EUCAIM creates a multi-layered defence against legal, ethical, and security risks. We rigorously align our framework with GDPR, the AI Act, and other relevant EU regulations, ensuring our processes meet or exceed established standards for health data protection, ethical research, and the deployment of trustworthy AI systems.

At the heart of these agreements stands our commitment to patient rights. By upholding the highest standards of privacy, security, and ethical conduct, we honour the autonomy and dignity of individuals whose data supports research and development within EUCAIM. We send a clear signal to society that our project is built on transparency, accountability, and respect for fundamental rights.

This robust legal and ethical foundation is essential not only for regulatory compliance, but also for fostering trust. As we move forward, these agreements affirm our dedication to protecting patient rights and ensuring all stakeholders—legal teams, researchers, and society—can be confident in the integrity and trustworthiness of EUCAIM.

2.4.2 Requirements for Health Data Users developing AI Tools, Use cases definition

It is possible to consider that an activity of data processing is related to the development of AI tools. In this context, it is necessary to clarify that all previous requirements outlined in section 2.4.1 are fully applicable. Consequently, this section focuses solely on the specific additional requirements that pertain to the use of health data for AI tool development and testing within EUCAIM.

It is essential to define the use case from the outset, as different rules and obligations may apply depending on its nature. A key element in this process is determining the Technology Readiness Level (TRL) of the application. Understanding the TRL clarifies whether the use case is intended for research purposes, aims at developing or testing a tool prior to its market entry, or involves the further development of an already commercialized tool. This classification is crucial for correctly identifying the applicable legal and ethical requirements, as well as for ensuring that each project phase aligns with the compliance framework established by EUCAIM and the broader regulatory environment.

For each use case within the development and deployment of artificial intelligence tools using health data, the legal specifications and compliance requirements can vary substantially. It is essential to define the use case precisely from the outset, as distinct rules and obligations apply depending on whether the activity is focused on academic research, pre-market development, or further improvement of a commercialized tool.

When artificial intelligence tools are developed for research purposes, the AI Act emphasizes the protection of fundamental rights and the assurance of strict adherence to ethical principles. In this context, the development process must prioritize the preservation of patient privacy, robust data security, and respect for the autonomy and dignity of individuals whose data is processed. The legal framework requires comprehensive ethical oversight, including Data Protection Impact Assessments (DPIA), ALTAI (Assessment List for Trustworthy Artificial Intelligence) evaluations, and, where appropriate, Fundamental Rights Impact Assessments (FRIA). These mechanisms ensure that research activities comply with both the General Data Protection Regulation (GDPR) and the AI Act, and that they foster transparency, human oversight, and accountability.

For AI tools intended for market use, the nature and risk level of the tool must be carefully evaluated. Depending on the classification and intended application, such tools may be subject to verification by a notified body or direct oversight by the European Commission. The AI Act establishes that high-risk applications, particularly those affecting patient safety or public health, require rigorous compliance with established standards and procedures. In addition to demonstrating lawful, ethical, and robust operation, developers must supply evidence of security compliance and document the mechanisms for human supervision and transparency. The AI Act also delineates the obligations for risk analysis and ongoing monitoring of AI systems to ensure they remain trustworthy and do not compromise user rights.

Furthermore, if an AI tool is classified as a medical device, it must comply with the Medical Device Regulation (MDR). This entails that the development, testing, and deployment processes are subject to a strict regulatory framework, including conformity assessments, clinical evaluations, and continuous post-market surveillance. Developers must ensure that the AI tool meets the technical and safety requirements outlined by MDR and that all documentation, risk management, and audit trails are maintained according to regulatory standards. Only by fulfilling these additional controls can the AI tool be authorized for use within the healthcare sector.

In summary, the legal and ethical landscape for AI tool development is highly dependent on the specific use case. Research-focused projects are governed by principles enshrined in GDPR and the AI Act, emphasizing rights protection and ethical conduct. Market-ready tools must be assessed for risk and may require external verification or oversight, while AI systems considered medical devices are subject to the comprehensive requirements of the Medical Device Regulation. This multi-layered approach ensures that all stakeholders can trust in the safety, legality, and ethical integrity of AI tools deployed in health research and care.

For this reason, in addition to meeting all requirements outlined in Section 2.4.1, it is imperative to establish close collaboration between EUCAIM's legal support and the legal teams of any entities operating under the scenarios described in this section. This joint effort ensures seamless compliance, anticipates potential challenges, and empowers all stakeholders to uphold the highest standards of legal and ethical responsibility throughout the AI development lifecycle.

2.5 Software providers on boarding workflows

The sharing of software resources, information systems, and artificial intelligence (AI) tools within collaborative frameworks such as EUCAIM introduces a spectrum of legal risks and

liabilities. These risks can impact software providers, EUCAIM as a coordinating entity, and end-users who interact with or deploy the technology. Addressing these considerations is critical for protecting all parties, ensuring compliance, and fostering trust in innovative health data applications.

Legal risks and liabilities in sharing software resources and AI systems are multifaceted and dynamic. By systematically addressing ownership and licensing, experimental risks, code transparency, AI literacy, and regulatory authorizations, providers, EUCAIM, and users can collaboratively uphold the highest standards of safety, legality, and ethical responsibility. Transparent communication, robust documentation, and ongoing education must be prioritized to mitigate risks and foster innovative, trustworthy applications of health data technology.

2.5.1 Users management and role played under GDPR

To safeguard personal data and foster an environment of trust, several critical measures must be implemented during software on boarding within EUCAIM. First, if any software manages health data users' personal data, transparency is required. EUCAIM and, crucially, the data subjects themselves must be fully informed about what data is collected, how it is processed, and under what conditions. This level of openness not only meets legal requirements but also promotes ethical stewardship of sensitive information.

Second, before any software is integrated or permitted to interact with EUCAIM's systems, clear evidence of full compliance with GDPR must be provided. This includes, but is not limited to, completion of a comprehensive Data Protection Impact Assessment (DPIA) if needed. The DPIA serves as a systematic evaluation of potential privacy risks and ensures that mitigation strategies are in place before data processing begins. This proactive approach is vital in preventing breaches and maintaining the integrity of personal data throughout the lifecycle of the AI tool. In circumstances where a Data Protection Impact Assessment (DPIA) is not mandated by law, a dedicated risk analysis must nonetheless be conducted. This analysis should be specifically oriented toward the preservation of fundamental rights and the assurance of robust security measures. By instituting such a demanding process, EUCAIM demonstrates a proactive commitment to protecting individual rights and minimizing risks, even in scenarios where formal DPIA requirements do not apply.

Third, prior to integration, it is essential for the software provider and EUCAIM to jointly define the GDPR status and responsibilities of the provider. If the provider is to act as a data processor under GDPR, it is necessary to formalize this relationship through a processor contract. This agreement should outline the scope of data processing, security measures, and the obligations of both parties, ensuring that all activities adhere to EUCAIM’s compliance framework as well as broader regulatory standards.

By rigorously applying these principles, EUCAIM can guarantee that all software resources not only fulfil legal and ethical obligations but also uphold the rights and expectations of data subjects in collaborative health data environments.

2.5.2 Secure processing environment integration

As a foundational principle, EUCAIM is expressly designated as a secure processing environment. Any software seeking acceptance and integration into EUCAIM’s infrastructure must unequivocally adhere to all technical and organizational requirements established to safeguard data integrity and system resilience. This includes, but is not limited to, strict

protocols for traceability of data flows and processing activities, robust mechanisms for incident response and timely data breach notification, and comprehensive risk management strategies addressing security threats unique to AI.

Accountability is central to this framework: software providers are expected to present verifiable evidence of the security measures implemented within their solutions. This encompasses documentation and, where applicable, third-party certifications that demonstrate compliance with EUCAIM's security standards. Providers must be prepared to promptly address any vulnerabilities, support forensic investigations, and cooperate fully in the event of an incident, ensuring that stakeholders' trust is maintained and that the integrity of both data and processing environment remains uncompromised.

2.5.3 Software ownership and licensing

It is essential to explicitly state whether a software product is proprietary, open-source, or distributed under specific reuse conditions—such as a Creative Commons License or equivalent alternative.

Proprietary software may entail restrictions on redistribution, modification, or use, often defined in End User License Agreements (EULA) or similar contracts. These restrictions must be made clear to users and to EUCAIM to avoid inadvertent breaches of intellectual property rights.

Open-source solutions, while generally more permissive, may still be governed by licenses that specify obligations (e.g., attribution, share-alike, or non-commercial clauses). Full transparency regarding these terms is vital to ensure lawful use and avoid downstream liabilities.

Where Creative Commons or similar licenses apply, the precise terms—such as rights to copy, modify, distribute, or use for commercial purposes—should be documented and communicated to all stakeholders.

2.5.4 Transparency about Code and business secrecy

Transparency regarding access to a software's codebase is an essential consideration for integration within collaborative environments like EUCAIM. Ideally, providers should make source code, architecture documentation, and revision histories readily available, fostering openness and trust among stakeholders. However, there are instances where complete transparency cannot be achieved, often due to the legitimate need to safeguard business secrets, intellectual property, or competitive advantages.

In such situations, it becomes crucial for providers to clearly articulate the legal or strategic grounds for limiting access to the code. This ensures that stakeholders are informed about the reasons behind these restrictions and can make decisions accordingly. Nevertheless, the absence of full disclosure does not preclude the necessity for independent validation. Providers ought to propose alternate avenues for scrutiny—such as third-party audits, external assessments, or certification schemes—that enable users and the wider community to retain a reasonable degree of confidence in the software's integrity and reliability.

By combining explicit communication about limitations with robust verification protocols, EUCAIM can continue to uphold its commitment to secure and trustworthy software integration, even in cases where business secrecy must be preserved.

2.5.5 Health data users, intellectual property rights, trade secrets and similar rights

Software integrated within EUCAIM has the potential to be employed in treatments pursuing innovative objectives characteristic of both research and entrepreneurial initiatives. Software providers must unequivocally guarantee the absolute neutrality of their applications, ensuring that under no circumstances will these tools be used to discover, appropriate, or repurpose any creations—of any kind—produced by a health data user within the EUCAIM ecosystem.

2.5.6 Risks associated with experimental software

When software is experimental or under development, potential risks arising from use must be disclosed in advance. This includes limitations in performance, accuracy, reliability, or security which may not yet be fully mitigated.

Providers are responsible for issuing clear warnings regarding the experimental nature of the software, including any adverse effects on data integrity, system stability, or possible unintended consequences in clinical or research settings.

2.5.7 Prior authorization and regulatory compliance

Medical Device Regulation and Documentation

- If the software or AI system falls under the Medical Device Regulation (MDR), it is subject to rigorous regulatory oversight prior to deployment.
- Providers must supply supporting documentation, including conformity assessments, clinical evaluations, and certification from notified bodies as required by MDR.
- EUCAIM should maintain a registry of authorized software, ensuring that only compliant systems are on boarded and made available for use in healthcare or research settings.
- Any updates or changes to the software must trigger a review of authorization status, with prompt reporting of new documentation or regulatory decisions.

2.5.8 Medical Device Regulation, AI Act compliance, and documentation

All software that is marketed—including but not limited to products intended for commercial use—must satisfy the relevant conditions set forth by both the AI Act and Medical Device Regulation (MDR). For EUCAIM, "marketed" refers broadly to any product that is released and considered "in production," regardless of its intended purpose or target audience.

Providers are required to supply comprehensive supporting documentation, including conformity assessments, clinical evaluations, and certification from notified bodies as mandated by MDR and the AI Act. Regulatory compliance must be assured before the software is on boarded or made available for use within healthcare or research environments.

EUCAIM should maintain a registry of authorized software, ensuring that only fully compliant and approved systems are released for operational use. Any updates or modifications to the software must trigger a reassessment of its authorization status, with prompt submission of new documentation and regulatory determinations as necessary.

2.5.9 AI literacy and informed usage

Article 4 of the AI Act mandates that users must be provided with sufficient and clear information regarding the use, capabilities, and limitations of artificial intelligence systems. This legal requirement ensures transparency, informed decision-making, and accountability in the deployment of AI technologies. As such, offering adequate details to users is not only a best practice but a compulsory obligation for compliance. This requires:

- To ensure adequate understanding of AI systems, sufficient information—collectively termed “AI Literacy”—must be provided to all users. It encompasses:
- The fundamental nature and intended functions of the AI system.
- Conditions and requirements for safe operation and integration.
- Detailed instructions on modes of use, including technical prerequisites and compatibility.
- Potential risks, limitations, and ethical considerations, particularly in relation to data privacy, bias, and decision-making transparency.

In accordance with the AI Act, it is essential to emphasize that in the case of High Risk AI Systems, transparency obligations are not optional but mandatory for deployment on the EUCAIM platform. Providers must ensure that all transparency requirements—including detailed disclosure regarding system functionality, intended use, inherent limitations, and risk factors—are fully met and clearly communicated prior to on boarding or operational release. These systems require heightened scrutiny and documentation to guarantee that users and stakeholders are equipped with all necessary information to support safe, ethical, and informed usage.

Providers should accompany software distribution with comprehensive user guides, risk assessments, and training resources to empower responsible adoption and use.

EUCAIM may facilitate workshops, webinars, or documentation repositories to strengthen AI literacy across its network and ensure harmonized standards of understanding.

ANNEX A: Data transfer checklist

This section summarises in a comprehensive table all the actions to be performed in the case of Health Data Holders that will upload their data into a reference node.

Action	Description	Documents
Provide documentation	- Proof of legal representative, and legal basis if necessary. - A copy of a favourable ethical approval (if applicable). - A report from the DPO confirming legal compliance. - Security compliance - GDPR compliance - Data Protection Impact Assessment (if applicable). - Any documents required under the national legislation. - Evidence of an adequate anonymization/pseudonymization process that has been carried out - Terms of Usage for the data.	D4.4 Final rules for participation report (See Sections 4.4.1 (Legal requirements) and 4.4.2 (Ethical requirements for Data Holders)
Data Transfer Agreement	Fill-in and sign the DTA.	Draft DTA
Get Familiar with EUCAIM	- Follow the EUCAIM training material and brief documents. - Browse architecture and - Watch webinars and videos.	- https://dashboard.eucaim.cancerimage.eu - https://eucaim.gitbook.io/end-user-guide - https://www.youtube.com/@EUCAIM - https://training.eucaim.cancerimage.eu/
Request a EUCAIM User	Request a EUCAIM User in the Dashboard.	Registration of users in EUCAIM
Extract the Imaging and clinical data	Use your own tools to extract the Medical Images and the clinical data.	N/A

Action	Description	Documents
Annotate the data (optional)	Use your own annotation tool or the one selected by EUCAIM (MITK). Convert the annotations into DICOM SEG.	- MITK (Medical Imaging Interaction Toolkit) Workbench - DicomSeg converter
Data de-identification	Ensure that no identifiable information is present in the dataset. If your imaging data are not already de-identified, you may use the EUCAIM Anonymizer.	EUCAIM Anonymizer
Re-identification risk assessment (optional)	Assess the risk of re-identification of patients based on your imaging metadata by checking hidden DICOM Tags.	Wizard
Data Quality assessment (optional)	You may check the accuracy and integrity of your imaging dataset.	DICOM File integrity checker
Provide Data Ingester Account Details	Open a ticket in the helpdesk, select the "Reference nodes" group (or "Technical support team" if unavailable) and add a request with the title: "Create a data ingestion project in UPV" or "Create XNAT project in HealthRI" (depending on the Reference site), providing the name of the project, the username in EUCAIM who will manage it. An answer will be given soon.	https://help.cancerimage.eu
Download and install the Data Ingestion tool	Download the Data Ingestion tool for the UPV node and the Clinical Trial Processor (CTP) for HealthRI.	- UPV Ingestion Tool - CTP.
Request a user in the Reference node	Choose the reference node where the data will be uploaded (only one): - UPV (login button, register through LS-AAI and ask for a "Data Ingester" account) - Health RI (XX)	Registration of users in UPV-eucaim-node, XXXX
Upload Imaging Data	Upload imaging data in the platform as described in the instructions (6.2.2 for UPV node and 6.2.3 for Health-RI).	User Guide for Data holders
Upload clinical Data	Once medical imaging data is uploaded, you can proceed with the clinical data. If the	- UPV Ingestion Tool

Action	Description	Documents
	process of converting the clinical data is expected to be long, we encourage you to create an “image-only” dataset by skipping this step. Use the same tool as before for UPV and XNATpy for Health-RI. Data can be in CSV or JSON.	- XNATpy
Create and Publish the Dataset	The dataset has to be created according to the instructions in the Gitbook (section 6.2.2.3 for UPV and 6.2.3 for Health-RI).	User Guide for Data holders
Provide the dataset’s metadata	Provide the metadata of the datasets according to the EUCAIM schema. In case of doubts with the terminology, use textual descriptions.	EUCAIM Dataset metadata or Molgenis excel template
Make a request of registry upload	Create a helpdesk ticket on the category catalogue, providing the spreadsheet file with the metadata information. The helpdesk team will contact you back informing if the dataset has been properly registered or requesting more information.	https://help.cancerimage.eu
Verify the entries in the catalogue	Access the registry in the catalogue and verify the collection.	https://catalogue.eucaim.cancerimage.eu/#/collection/<<identifier>>

ANNEX B: Data sharing checklist

This section summarises in a comprehensive table all the actions to be performed in the case of Health Data Holders that will deploy a federated node.

Action	Description	Documents
Provide documentation	- Proof of legal representative, and legal basis if necessary. - A copy of a favourable ethical approval (if applicable). - A report from the DPO confirming legal compliance. - GDPR compliance - Data Protection Impact Assessment (if applicable). - Evidence of an adequate anonymization/pseudonymization process that has been carried out - Documents demonstrating the security of the information system. - Any documents required under your national legislation.	D4.4 Final rules for participation report (See Sections 4.4.1 (Legal requirements) and 4.4.2 (Ethical requirements for Data Holders)
Data Sharing Agreement	Fill-in and sign the DSA.	Draft DSA
Define especial Access Conditions	A Document to be signed by the Data User that indicates the conditions under the Data User can access the data.	Draft Template
Contact point for the negotiation (Only in federated nodes)	The LS-AAI details of the data holder delegate who will interact with the Data User through the negotiator.	Registration of users in EUCAIM LS-AAI.
Get Familiar with EUCAIM	- Follow the EUCAIM training material and brief documents. - Browse architecture and - Watch webinars and videos.	- https://dashboard.eucaim.cancerimage.eu - https://eucaim.gitbook.io/end-user-guide - https://www.youtube.com/@EUCAIM - https://training.eucaim.cancerimage.eu/

Action	Description	Documents
Setup your local node	Deploy a node to host data and services to reach the desired interoperability level.	Section 3.7 in D5.6
Request a EUCAIM User	Request a EUCAIM User in the Dashboard.	Registration of users in EUCAIM
Extract the Imaging and clinical data	Use your own tools to extract the Medical Images and the clinical data	N/A
Annotate the data (optional)	Use your own annotation tool or the one selected by EUCAIM (MITK). Convert the annotations into DICOM SEG.	- MITK (Medical Imaging Interaction Toolkit) Workbench - DicomSeg converter
Data de-identification	Ensure that no identifiable information is present in the dataset. If your imaging data are not already de-identified, you may use the EUCAIM Anonymizer-	EUCAIM Anonymizer
Re-identification risk assessment (optional)	Assess the risk of re-identification of patients based on your imaging metadata by checking hidden DICOM Tags.	Wizard
Data Quality assessment (optional)	You may check the accuracy and integrity of your imaging dataset	DICOM File integrity checker
Set up of the local catalogue	Deployment of a local instance of the catalogue.	Gitlab repository
Population of the data	Data should follow the EUCAIM interoperability schema.	- Sample file with the schema - End User Guide
Federation of the catalogue **(in progress)**	Enable automatic synchronisation of the local catalogue with the central one.	In progress
Metadata mapping	A mapping of the searchable items to the local variables should be defined.	Tables 14 and 15 in D5.6

Action	Description	Documents
Development of Mediator Component	Develop a mediator to connect the local searching API with the federated explorer.	Section 5.2.1 Dataset in a Federated Node, subsection “Guidelines for creating a mapping component” in D5.6
Deployment of the Mediator Component	The deployment of a mediator component can be done as a Docker container. Deploy the additional components of the Federated Search.	Section 5.2.1 Dataset in a Federated Node in D5.6
Request registration in the federated explorer	Request the connection of the central instance of the federated search through a ticket in the helpdesk.	https://help.cancerimage.eu
Deploy a federated computing node	Request technical support to the technical team through the helpdesk.	https://help.cancerimage.eu

ANNEX C: Data Access checklist

Action	Description	Documents
Provide documentation	- Proof of legal representative - A report from your DPO confirming legal compliance. - A copy of a favourable ethical approval (if applicable). - GDPR compliance - Data Protection Impact Assessment, if applicable. - Security Compliance - AI Impact Assessment (ALTAI and FRIA), if applicable - Additional documentation required under the national law. - AI Literacy - Software ownership and licensing - Medical Device Regulation Authorisation, if applicable.	- F&A template - Template DPO statement
Request a EUCAIM User	Request a EUCAIM User in the Dashboard.	Registration of users in EUCAIM