

CA20104 – Network on evidence-based physical activity in old age (PhysAgeNet)

Deliverable D2.1

*D2.1 Compendium of legal, ethical and resource aspects for open data
repositories*

Contributors

Working Group 2

Carl-Philipp Jansen (WG2 co-leader), Tiia Kekäläinen (WG2 leader), Svava Sigurðardóttir (WG2 member), Alice Masini (WG2 member), Erja Portegijs (former WG2 leader, active member)

Participants in the expert discussions and review groups have contributed to these results.

Table of Contents

1. Introduction.....	3
2. Ethical considerations in data sharing.....	5
2.1. Introduction and key ethical principles.....	5
2.2. Informed consent, participant rights, and data anonymization.....	6
2.3. Ethical review and oversight.....	7
3. Best Practices and Recommendations.....	8
4. Resource Considerations in Data Sharing.....	9
4.1. Infrastructure requirements, budgeting, and data management.....	9
4.2. Data management costs.....	10
5. Conclusion.....	11
6. References.....	12

1. INTRODUCTION

In recent times, the provision of access to data for scientific purposes has gained increasing importance, but also complexity. Data sharing plays a crucial role in health research by enhancing collaboration, improving efficiency, and fostering innovation. However, effective data sharing requires careful navigation of legal, ethical, and resource-related challenges. The implementation of regulatory mandates, internal procedures, and technical processes to enable data provision is challenging. As a result, this task is often delayed and inefficient in most projects. Standardised procedures for this matter could foster data sharing procedures and create higher impact and efficiency.

Data sharing is integral to modern health research as it enables:

- Greater collaboration and efficiency across projects.
- Enhanced research impact by allowing broader analysis of large datasets.
- Improved patient outcomes by leveraging shared data to develop innovative treatments and solutions.

However, data sharing introduces legal, ethical technical, and resource aspects and complexities that must be addressed.

According to Horizon Europe, data should be deposited as soon as possible after its creation and no later than the project's completion. However, additional requirements apply:

- Data supporting a scientific publication must be deposited no later than the time of publication, following standard community practices.
- In the event of a public emergency, and upon request from the granting authority, immediate open access must be provided. If open access exceptions apply, the data should still be made available to legal entities that require it to address the emergency.
- In exceptional circumstances, data may be deposited after the project's conclusion.

This report is being written under thorough consideration of the following documents:

„Data Sharing Playbook“, issued by the European Federation of Pharmaceutical Industries and Associations (EFPIA), 2022;

OpenAIRE's guide for researchers on „How to find a trustworthy repository for your data“ ([How to find a trustworthy repository for your data](#));

OpenAIRE's „A Research Data Management Handbook – A primer on managing your research data“ (<https://www.openaire.eu/rdm-handbook>);

2. LEGAL CONSIDERATIONS IN DATA SHARING

The content of Chapter 2 was contributed by external legal experts who are not affiliated with PhysAgeNet.

2.1. Introduction and Purpose of the Framework

Working Group 2 has launched an initiative, WG2, and identified the need to assess the legal framework for sharing research data about technology-assisted physical activity for older persons. The objective is to determine the conditions under which research data can be openly shared for use by other researchers within the EU.

The aim is to establish a data repository on an existing platform where researchers can share gathered research data and access datasets shared by other researchers. The need to separately assess the sharing of pseudonymized and anonymized data has been identified. Additionally, it has been noted that the research data is likely to include health data.

This framework describes the main considerations for openly sharing research data within the EU. It should be emphasized that the framework does not provide detailed instructions, and member states participating in the EU COST Action network must take into account the requirements arising from national laws in each case.

2.2. Scientific Research Purposes in the Context of the General Data Protection Regulation (GDPR) and the Treaty on the Functioning of the European Union (TFEU)

The General Data Protection Regulation (GDPR) does not precisely define “scientific research purposes”, but Recital 159 states that *“the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area.”*

Article 179(1) of the Treaty on the Functioning of the European Union (TFEU) states that *“The Union shall have the objective of strengthening its scientific and technological bases by achieving a European research area in which researchers, scientific knowledge and technology circulate freely, and encouraging it to become more competitive, including in its industry, while promoting all the research activities deemed necessary by virtue of other Chapters of the Treaties”*.

Based on the provisions, it appears that the initiative falls within the scope of “scientific research purposes”. The described research can be interpreted as contributing to the advancement of technological development, or as either fundamental research or applied research, as outlined in Recital 159 of the GDPR. Additionally, it should be noted that the scope of scientific research is broad pursuant to the GDPR. From the perspective of the TFEU, the described research is specifically intended to promote EU-wide research, which aligns with the objectives stated in Article 179(1) of the TFEU.

However, in this case, data is being shared on a research platform, rather than being used solely by the controller for their own scientific purposes. This requires that various obligations under the GDPR are taken into account, depending on the specific circumstances (such as roles of the parties).

2.3. General Data Protection Regulation

Below is a high-level list of the requirements of the GDPR that must at least be considered when sharing the research data in the context of the initiative.

i. GOVERNANCE, ACCOUNTABILITY AND DATA PROTECTION BY DESIGN

Data controller:

- **Responsibility for data collection and data sharing:** Determine who is the data controller and thus responsible for the collection and sharing of research data. It is possible that there is one or several independent data controllers or joint controllership (e.g., between universities or research organizations).
- **Collaboration Between Data Controllers:** When data is shared between universities or research organizations, both collaborating parties are responsible for their respective data processing activities if they act as data controllers. This entails:
- Establishing agreements on data processing terms (e.g., a data transfer agreement or joint controller arrangement).
- Clearly documenting the data-sharing process and its purpose.

Relevant provisions: Articles 4, 5, 24, 26 of the GDPR.

The role of the platform administrator(s):

- **Responsibilities and duties:** Clearly define responsibilities and duties of platform administrator(s) for ensuring secure processing and sharing of data.
- **Access to the data:** Monitor who has access to the data and how it is being used.
- **Role(s) of the platform administrator(s):** Define the role of the platform administrator from a data protection perspective (data controller or data processor). If you transfer data to data processor, a data processing agreement is required (Article 28 of the GDPR). If you act as a joint controller with other controller(s), you shall in a transparent manner determine your respective responsibilities (Article 26 of the GDPR).

Relevant provisions: Articles 4, 5, 24, 26, 28 and 32 of the GDPR.

Accountability and documentation:

- **Documentation:** Document all data processing activities, including the sharing of data among researchers.
- **ROPA:** Conduct a Record of Processing Activities (ROPA) where applicable.

Relevant provisions: Articles 5, 24, 28, 30 and 32 of the GDPR.

Data protection by design:

- **Supporting GDPR requirements:** The platforms and processes used for sharing data must support GDPR requirements (such as data protection principles outlined in Article 5).
- **Development phase:** Practical measures and technical solutions should be implemented during the development phase.
- **Secure access to the data:** Use platforms that enable secure access to the data.

Relevant provisions: Articles 5, 25 and 32 of the GDPR.

ii. LEGAL BASIS AND PURPOSE OF PROCESSING

Grounds for processing personal data:

- **Original Legal Basis:** Ensure that the initial data collection is based on a lawful ground for processing (e.g., consent or public interest in scientific research, Art. 6(1)(e) or Art. 9(2)(j)).
- **Legal Basis for Further Use:** If the data is shared for use in new research purposes, this may require a new legal basis for processing, unless
 - the original legal basis also covers further use or
 - it can be interpreted that the further processing for scientific research purpose is compatible with the purpose for which the data was initially collected (see e.g., Recital 50 of the GDPR).

Relevant provisions: Articles 6 and 9 and Recital 50 of the GDPR.

Purposes of data processing and purpose limitation:

- **Original legal basis:** The original purpose for processing personal data must be compatible with the purpose of further processing.
- **Legal basis for further use:** The GDPR's Recital 50 acknowledges that further processing of personal data for scientific research purposes is generally considered compatible with the original purpose, if:
 - The further use remains within the limits of scientific research purposes.
 - The further processing complies with the GDPR's requirements and includes necessary safeguards (Art. 89(1)).

Contractual arrangements: Agree in writing with other researchers that the research data may only be further used for scientific research purposes.

Relevant provisions: Article 5(1)(b) and Article 89(1) and Recital 50 of the GDPR.

iii. DATA SECURITY AND PROCESSING SAFEGUARDS

Anonymization and pseudonymization:

- **Anonymization:** If the research data is fully anonymized, the GDPR does not apply (see Recital 26 of the GDPR). However, it must be noted that the concept of anonymization must be interpreted strictly, which means that the data cannot be restored to an identifiable form, even with the use of additional tools, to be considered anonymized.

- **Pseudonymization:** If the data is pseudonymized but individuals remain identifiable, the GDPR applies. In this case, adequate technical and organizational safeguards, particularly those ensuring data minimization, must be ensured (Article 89(1) of the GDPR).

Relevant provisions: Article 89(1) and Recitals 26 and 156 of the GDPR.

Access control, terms of use and security measures:

- **Access control:** Platforms used for data sharing must include access control (e.g., role-based permissions).
- **Terms of use:** If data is shared on open research platforms, clearly define its terms of use and ensure that the data remains limited to scientific purposes.
- **Encryption:** Encryption of data during transfer and storage must be implemented.

Relevant provisions: Articles 5 and 32 and Recital 83 of the GDPR.

iv. CONSENT AND RIGHTS OF DATA SUBJECTS

Consent:

- **Clear and documented consent:** Ensure that clear and documented consent has been obtained from participants for sharing their data for research purposes, especially for possible further use by other researchers.
- **The scope and main requirements of consent:** The consent must cover data sharing within the EU and the specific purposes of processing. Even though the scientific research purpose is interpreted as compatible with the original purpose under the GDPR (see e.g., Recital 50), consent must be broad enough to include data sharing and possible data reuse. Consent must be voluntary, specific, informed, and unambiguous. Consent may be given in writing, electronically, or in another form that clearly documents it.
- **The withdrawal of consent:** The data subject shall have the right to withdraw his or her consent at any time. This right must be communicated clearly to participants during the consent process. For pseudonymized or identifiable data, procedures must be in place to address withdrawal requests effectively. If the data has been anonymized, withdrawal is no longer applicable.

Specific challenges in research contexts:

- **Identifiable data:** When sharing identifiable data, the right to withdraw consent at any time poses practical challenges, especially if the data has already been shared or reused.
- **Anonymized data:** If the data is anonymized, consent may not be required, as anonymized data falls outside the scope of the GDPR. However, strict anonymization standards must be met to ensure that re-identification is not possible.

Relevant provisions: Articles 4(11) and 7 and Recitals 32, 42, 50 of the GDPR.

Special categories of personal data:

- **Explicit consent:** If special categories of personal data are processed, the consent must be explicit (GDPR, Article 9 (2)(a)) in addition to the other requirements for consent (GDPR, Article 4 (11); Article 6(1)(a) and Article 7).

Relevant provisions: Articles 4, 6, 7 and 9 of the GDPR.

Rights of the data subject:

- **Rights of the data subject:** Ensure that the rights of the data subject can be exercised (e.g., the right to access, rectify, or object to the processing of their data) pursuant to Articles 12-22 of the GDPR.
- **Exceptions for the rights of the data subject:** EU or member state law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 12 of the GDPR.

Relevant provisions: Articles 12-22 and 89(2) of the GDPR.

Informing data subjects:

- **Informing data subjects:** Data subjects must be informed in clear and understandable manner that their data is being collected and further shared for research purposes.
- **Content of communication:** Communication should emphasize how data is processed (description of processing activities) and what rights data subjects have. Additionally, data subjects should be informed how their data is protected.

Relevant provisions: Articles 12-14, 15-22 and 32 of the GDPR.

v. OPERATIONAL REQUIREMENTS

Organizational requirements (policies, guidelines, etc.):

- **Guidelines:** Establish clear organizational guidelines or policies on how data is shared responsibly and lawfully.
- **Documentation:** Document practices related to data sharing, particularly among EU researchers.

Relevant provisions: Articles 24, 25 and 89(1) of the GDPR.

Data lifecycle:

- **Data retention and deletion:** Define how long the data (including backups) will be retained and when it will be deleted.
- **Data deletion:** Deletion practices must be clear and documented.
- **Exception for longer retention periods:** Personal data may be stored for longer periods insofar as the personal data will be processed solely for, for example, scientific research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures.

Relevant provisions: Article 5 of the GDPR.

vi. DATA TRANSFERS

Data transfers:

- **Contractual arrangements:** Use data protection agreements or other formal arrangements among researchers if needed. Ensure that data protection and data security are implemented in data transfers.
- **Safeguards for data transfers:** If data is processed within the EU/EEA, safeguards for international data transfers are not required. If data is transferred outside the EU/EEA (e.g., the platform operator processes data in a third country), there must be an appropriate safeguard for the transfer (e.g., Standard Contractual Clauses (SCCs)).
- **Openly available data:** If the data is openly available without restrictions based on location, it can be presumed data is transferred outside EU/EEA. If the data contains personal data, the Data Controller is obliged to assess that it has a right to transfer the data as well as to assess risks based on the recipient's country/area. In cases where data is openly available it might be hard to control and assess all the areas and their legislation where the data could be transferred. If the access to data is restricted to EU/EEA and/or it is anonymized efficiently so that it no longer is considered personal data, these obligations on data transfers don't apply.

Relevant provisions: Articles 5, 26 and 28 of the GDPR.

Third-party processors:

- **Contractual arrangements:** If third parties (e.g., platform administrators or service providers) are involved in data sharing, ensure in writing that they comply with GDPR requirements.

- **Data processing agreements:** Ensure that there are relevant data processing agreements conducted with third parties.

Relevant provisions: Articles 28, 32 and 46 of the GDPR.

vii. DATA BREACH MANAGEMENT

Data breach management:

- **Plan for data breaches:** Develop a plan for detecting, reporting and managing potential data breaches. Ensure that data breaches can be notified within the 72-hour timeframe.
- **Collaborative process:** Assess the possibility for collaborative process for addressing data breaches.

Relevant provisions: Articles 26, 28 and 32-34 of the GDPR.

viii. DATA PROTECTION IMPACT ASSESSMENT

- **Data protection impact assessment (DPIA):**
- **A high risk to data subjects' rights:** If data sharing poses a high risk to data subjects' rights, a DPIA may be required.

Relevant provisions: Article 35 and Recitals 84, 90 and 92 of the GDPR.

ix. DATA PROTECTION OFFICER (DPO)

Data protection officer:

- **Designation of the data protection officer:** Data protection officer must be appointed if you:
 - process sensitive data on a large scale
 - monitor individuals regularly, systematically and on a large scale or
 - your organization is a public authority.

Relevant provisions: Article 37 of the GDPR.

2.4. Other Regulations and Frameworks

Data Act: This regulation supports research collaboration by facilitating access to private sector data and defining the conditions for data sharing. Its impact on data sharing between researchers is minimal unless the research involves using commercial data sources.

AI Act: The AI Act introduces requirements that must be considered if data processing involves AI-based solutions. In such cases, researchers/universities/research organizations must ensure compliance with the Act's provisions on transparency, data quality, and risk management. This is particularly relevant if shared datasets are used to develop AI systems, especially those classified as high-risk, which require additional documentation and safeguards.

Open Data Directive: This directive promotes the reuse of public sector information. If research data is publicly funded, it may be encouraged to open access for other researchers. In such cases, anonymization is a critical tool to enable openness while complying with GDPR.

European Health Data Space (EHDS): The EHDS will be especially relevant for sharing health data. If research data includes health-related information, EHDS may provide a standardized infrastructure for sharing it across the EU in the future. This will be crucial for researchers engaged in multinational studies.

2.5. Sharing of Pseudonymized Data

Pseudonymized data is still considered personal data under the GDPR, meaning that the regulation fully applies. The sharing of pseudonymized data for scientific purposes requires implementing appropriate technical and organizational safeguards, such as access controls, data minimization, and encryption. Additionally, the data controller must ensure that the data cannot be re-identified without additional information that is kept separately under strict security measures. Transparency is critical, and data subjects must be informed that their pseudonymized data may be shared for further research purposes. Sharing pseudonymized data across borders within the EU is generally allowed if these safeguards are in place.

However, the Court of Justice of the European Union (CJEU) has assessed the concept of pseudonymized data in its judgment *T-557/20 - SRB v EDPS*. The CJEU held that pseudonymized data is not considered personal data unless the recipient has legal means practically enabling it to access the additional information necessary to re-identify the individuals.²

See *SRB v. EDPS* (T-557/20, 26 April 2023), para. 105.

The case highlights the importance of context and the recipient's circumstances when evaluating whether the data is considered pseudonymized or non-personal data. In the context of the initiative, the classification of research data depends on whether the platform or its administrators or other recipients of data (e.g, researchers, universities, research organizations) have legal and practical means to access additional information enabling re-identification of individuals. If any of the recipients cannot practically re-identify the data without additional information it does not have access to, the pseudonymized data may not be considered personal data under GDPR. The research data can be considered personal data for some recipients but not for others, depending on the specific recipient's ability to identify individuals using the data, either alone or in combination with additional information to which they have access.

2.6. Sharing of Anonymized Data

Sharing anonymized data generally falls outside the scope of the GDPR, as anonymization ensures that data subjects cannot be identified, even indirectly or with the use of additional information. For research purposes, sharing anonymized data is a preferred option because it eliminates the risk of re-identification while enabling broad data accessibility. However, the process of anonymization must meet strict criteria to ensure that re-identification is impossible under all reasonably foreseeable circumstances. Researchers and data controllers should carefully document the anonymization process to demonstrate compliance with the GDPR's

standards and ensure data security throughout its lifecycle. Anonymized data can be shared without the same legal restrictions, facilitating open access to research data while protecting the privacy of individuals.

2.7. Local legislation compliance

While the GDPR provides a unified framework for data protection across the EU, individual member states may impose additional requirements for the processing and sharing of research data. Article 89(2) of the GDPR allows member states to introduce more specific provisions regarding scientific research, particularly for safeguarding personal data and balancing data subjects' rights with the needs of research. For example, some countries may require prior ethical approvals, restrict certain types of data sharing, or impose stricter rules for health data.

When sharing research data across the EU, it is essential to evaluate and comply with the national laws of each member state involved. For example, in Finland, Section 31 of the Data Protection Act includes specific requirements for the processing of personal data for scientific research purposes.

Universities and research organizations must account for variations in legal requirements, such as obligations for pseudonymized data or conditions under which anonymized data is deemed sufficient for sharing. Collaboration with legal experts or data protection authorities in each jurisdiction may be necessary to ensure compliance with both GDPR and local legislation.

2.8. Summary

This framework provided general guidance on how research data in the context of the initiative may be shared among researchers across the EU. The GDPR is regarded as the most relevant and significant regulation concerning the sharing of research data. While the scientific research purpose is generally deemed compatible with the original purpose for which the data was processed, it is crucial to ensure that any further use is strictly limited to scientific research purposes.

To comply with GDPR, it is essential to implement appropriate safeguards, such as anonymization or pseudonymization of data, and to ensure transparency regarding data processing practices. The anonymization of personal data in research datasets would mean that the requirements of the GDPR would not generally need to be followed. However, it is important to note the key criteria for anonymized data. Furthermore, as the judgment *T-557/20 - SRB v EDPS* by the CJEU illustrated, pseudonymized data may, under certain circumstances, also be considered non-personal data.

Researchers and organizations must also carefully consider the principles of data minimization and purpose limitation, in particular, to uphold the rights and freedoms of data subjects.

3. ETHICAL CONSIDERATIONS IN DATA SHARING

3.1. Introduction and key ethical principles

Sharing research data and establishing open data repositories on technology-assisted physical activity intervention for older persons within the EU COST Action network PhysAgeNet, presents opportunities and *benefits* but can also involve challenges. One of the Deliverable D2.1 objectives is to assess ethical aspects for open data repositories and for that purpose ethical considerations and key ethical principles in data sharing are introduced, to highlight potential benefits and challenges.

The main motivation for researchers to share their data relates to both individual and collective benefits. Data sharing promotes *openness*, *transparency*, and *accountability* in research, which are important ethical principles of research, and to discovery of researchers' datasets and research results. Sharing data with others for scientific purposes can both benefit the researchers themselves and the research community. Furthermore, data sharing based on *social responsibility*, and contributions to large datasets that enable broader analysis, can provide important information that can benefit society, for example as useful guidance in policymaking or for innovative solutions in healthcare.

Data sharing, access to shared datasets, and research collaboration in the EU Cost Action network can therefore promote further research into evidence-based technology supported activities for the elderly, as well as new treatment solutions with the aim of improving *quality* of healthcare and outcomes for patients.

An important aspect related to data generated from research on human, as in this study on technology-assisted physical activity intervention for older persons, is that data exists due to the participation of individuals in research. A possible incentive for participating in research is mutual responsibility in the creation of general knowledge for better healthcare. Notwithstanding and without diminishing the importance of individual and collective benefits of research, there might be potential risks related to research data collection and data sharing, known as *privacy risk*, that could cause *informational harm*, and in that regard is important to store data in Trustworthy Digital Repository (TDR) to protect the data and foster *trust*.

Data protection is a core issue in the European Union (EU), and it is a fundamental personal right related to human dignity and the ethical principles *autonomy*, *nonmaleficence* and *justice*. Data protection and *confidentiality* are important conditions in research to protect data subjects' *privacy*.¹

¹ Ethics and data protection, p. 11:

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_en.pdf

Data generated in research projects funded by the EU should take FAIR principles into account, and be “as open as possible, as close as necessary”² which refers to assessment of benefits and challenges of the data sharing. Despite the emphasis on EU regulations, it should also be emphasized that researchers in the EU COST Action network must always follow their national regulations and understand that rules may differ between countries.

3.2. Informed consent, participant rights, and data anonymization

Ethical principles in data sharing ensure the protection of participants' rights and the responsible use of data.

Informed consent is a key concept in research ethics and its moral dimension includes respect for human dignity, protecting the rights of participants and promoting their autonomy.³ Informed consent should be context specific and clearly defined to distinguish between type of research, and the use of data. Participants should be informed about what data will be collected and how it will be used during and following the study, to ensure transparency on the use of research data.

Informed consent should be clearly defined to distinguish between consent for trial participation vs. consent for data sharing. Organizations must ensure that consent allows for secondary data use in research while maintaining participant autonomy.

If the intention is to use primary data in future research or share the data with others, it is fair and transparent to explicitly state it in the consent process and give the participant an opportunity to either consent to the secondary use of data, or opt-out of further use.⁴ It respects the participant's right to self-determination, and gives opportunity for shared responsibility.

The term *broad consent* has been used for consent form of further use of data, when the participant gives permission for continued use beyond the original study. In this context, research ethics committees can be important safeguards for the interests of data subjects, because participants usually cannot protect their own rights themselves in future (secondary data) studies, i.e., give approval themselves in the future research. Data subjects might lack control and insight of how the data are used in future research.

² Open science: https://rea.ec.europa.eu/open-science_en

³ Ethics and data protection, p. 11:
https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf

⁴ Ethics and data protection, p. 12:
https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf

To address this, information should be clear, and transparency ensured– to clearly and fairly explain that data are identifiable and personal during the study, but when it is over the data will be made anonymized, saved in a trustworthy repository, and then open for responsible use in further research.

Anonymization and pseudonymization are essential techniques to protect privacy while enabling data sharing. Fully anonymized data is easier to share as consent for further use is not necessary, but anonymization can limit research utility, among other things because it is difficult to link different data about an individual together.

The SAFE Data Standard (Sharing Anonymized and Functionally Effective Data Standard) proposes functionally effective anonymization while preserving data quality. It is a framework designed to facilitate the secure and ethical sharing of rich clinical trial data while preserving both data utility and privacy. The standard ensures that anonymized datasets remain functionally effective for research, meaning they retain statistical integrity and scientific validity while complying with data protection regulations like the GDPR.

Key principles of the SAFE Data Standard include:

- **Security Measures:** Implementing encryption, controlled access, and audit trails to protect data.
- **Anonymization:** Removing or altering identifying information to prevent re-identification.
- **Functionality:** Ensuring that anonymized data remains useful for scientific analysis.
- **Ethical Compliance:** Aligning data-sharing practices with regulatory requirements and participant consent.

By adopting the SAFE Data Standard, organizations can maximize the research potential of shared datasets while safeguarding privacy and fostering trust in data sharing initiatives.

Challenges that researchers in the study on technology-assisted physical activity intervention for older persons might need to respond to is reduced physical and/or mental capacity of participants, lack of health-, digital-, and technological literacy, and impaired cognitive competence, which can affect understanding and decision-making in the consent process, and in the research.

3.3. Ethical review and oversight

Researchers in EU COST Action network PhysAgeNet are encouraged to familiarize themselves with national regulation and requirements on ethical review related to open data sharing, which may vary by country.

Ethics committees should oversee data sharing policies to ensure compliance with ethical standards. Transparency in data sharing decisions fosters public trust and encourages participant engagement. Organizations must balance commercial interests with the ethical responsibility of

ensuring data accessibility for the public good. Ethical frameworks should promote non-discriminatory access to research data. Lesson learned from ethics review boards provided important guidance for ongoing review of research using personal data.

In studies that need approval from ethics committees, there should be information in the research plan about *data collection and use*. Researchers provide all necessary information about the data use, and that should include data sharing in the future. Ethics committees assess risks to data subjects in the context of benefits for science and society, and potential risks associated with data sharing and open data repository is primarily privacy risks that can cause informational harm. Confidentiality and data protection are key principles in responding to such potential harm and for respecting the privacy of data subjects.

4. BEST PRACTICES AND RECOMMENDATIONS

Early stakeholder involvement

- Engage legal, ethical, and resource experts early in the project to prevent delays.
- Identify key decision-makers and involve them in negotiations from the outset.
- Provide training on responsible data handling and sharing.

Clear and standardized documentation

- Use pre-approved templates for agreements to reduce administrative burden.
- Maintain detailed data flow diagrams to clarify processing roles.

Proactive risk mitigation

- Address potential GDPR conflicts and IP concerns before formalizing data-sharing agreements.
- Transparency about planned data sharing and open data repositories at the beginning of research if possible, and explicitly explain the use of data in the consent process.
- Adopting the SAFE Data Standard: security measures, anonymization, functionality, and ethical compliance – to maximize research potential while safeguarding privacy.
- Develop contingency plans to handle unforeseen challenges.

Promoting a data-sharing culture

- Organizations should cultivate an internal culture that values data sharing and recognizes its benefits.
- Transparency and mutual agreements among stakeholders will ensure efficient collaboration.
- Trustworthy Digital Repository (TDR) for data protection to foster trust and respecting privacy.
- Use cloud-based or decentralized storage for scalability and accessibility.
- Implement APIs for automated and efficient data exchange.
- Monitor network bandwidth to prevent slowdowns or bottlenecks.
- Ensure system interoperability to facilitate seamless integration.

5. RESOURCE CONSIDERATIONS IN DATA SHARING

Efficient resource allocation ensures that data-sharing initiatives are sustainable and cost-effective.

5.1. Infrastructure requirements, budgeting, and data management

With regards to infrastructure and technology requirements, organizations must select an appropriate data-sharing model:

- Centralized Model: A single repository for data storage.
- Federated Model: Distributed data access without centralizing storage.
- Hybrid Model: A mix of both approaches.

Standardized common data models and existing platforms should be leveraged to avoid unnecessary duplication.

With regards to budgeting and cost management, infrastructure costs for secure data storage, legal and compliance costs (e.g., GDPR assessments, legal counsel), and personnel costs for data governance and security management must be considered.

Developing a Data Management Plan (DMP) ensures clarity on data-sharing workflows. Within this task, roles should be assigned for data governance oversight (e.g., Data Protection Officers), legal compliance (e.g., contract managers), and IT and security (e.g., cybersecurity experts).

According to the Research Data Management Handbook, a DMP briefly defines:

- how the data will be created;
- how it will be documented;
- who will be able to access it;
- where it will be stored;
- who will back it up;
- whether (and how) it will be shared and preserved.

Data-sharing initiatives must adhere to recognized security standards to mitigate risks. Therefore, organizations should implement access control mechanisms (e.g., role-based access), encryption techniques for data transmission, and audit trails to monitor data access and compliance.

Long-term data sustainability strategies should be embedded in project planning, whereas public-private collaboration can enhance resource availability and long-term data access.

5.2. Data management costs

Proper planning for data management and sharing is essential, as these activities require both time and resources. Early planning can help minimize costs. Expenses related to open access for research data can be considered eligible costs, for example under a Horizon 2020 grant, provided they meet the conditions outlined in the respective Grant Agreement. Generally, this means they must be budgeted in advance and approved in the grant proposal, and they can only be claimed during the project's duration.

As an example, under <https://www.openaire.eu/how-to-comply-to-h2020-mandates-rdm-costs> a tool is provided to estimate costs for research data management. A four-step approach is advised (see link above):

“Step 1: Check the data management activities in the table and tick those that may apply to your proposed research.

Step 2: For each selected activity, estimate the additional time and/or other resources needed and cost this, e.g. people's time or physical resources needed such as hardware or software. Find out which resources, e.g. for data storage and backup, are available to you from your institution. Consider whether you need a dedicated data manager.

Step 3: Add these data management costs to your research application. Coordinate resourcing and costing with your institution, research office and institutional IT services.

Step 4: Plan the data management activities in advance to avoid them competing with the need to focus on research excellence.“

6. CONCLUSION

Legal, ethical, and resource-related considerations are fundamental to successful data sharing. By establishing clear legal frameworks, ensuring ethical compliance, and optimizing resources, organizations can create robust, sustainable, and impactful data-sharing initiatives. Proactive planning and adherence to best practices will facilitate seamless collaboration, enhance research impact, and foster trust among stakeholders.

7. REFERENCES

„Data Sharing Playbook“, issued by the European Federation of Pharmaceutical Industries and Associations (EFPIA), 2022.

OpenAIRE’s guide for researchers on „How to find a trustworthy repository for your data“ ([How to find a trustworthy repository for your data](#)).

OpenAIRE’s guide for researchers on „How to identify and assess Research Data Management (RDM) costs“ (<https://www.openaire.eu/how-to-comply-to-h2020-mandates-rdm-costs>).

OpenAIRE’s „A Research Data Management Handbook – A primer on managing your research data“ (<https://www.openaire.eu/rdm-handbook>).

Ethics and data protection, p. 11:

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf

Open science: https://rea.ec.europa.eu/open-science_en

Ethics and data protection, p. 11:

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf

Ethics and data protection, p. 12:

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf

Ethics and data protection, p. 11:

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf

Ethics and data protection, p. 12:

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf