Ref. Ares(2024)9279405 - 30/12/2024

XpanDH

Expanding Digital Health through a pan-European EHRxF-based Ecosystem

D1.9 – (D1.5.3) Updated Ethics and Data Management Plan

WP1 – Coordination

30.12. 2024

Authors:

Name	Organisation	Name	Organisation
Petra Wilson	IHE		
Anderson Carmo	ISCTE		

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HaDEA. Neither the European Union nor the granting authority can be held responsible for them.

Document control	
Status	Final
Version	1.0
Type of Document	R: Document, report;
Dissemination Level	PU – Public
Work Package	WP1 – Coordination
Full document name	D1.9 – (D1.5.3) Updated Ethics and Data Management Plan
Link to access document	N/A
Partner lead(s)	ISCTE
Other partners involved	HL-7, EMP, IHE- EUR, UNINOVA, ECHA, I~HD
What did this document aim to achieve?	This document provides the Data Management Plan for the XpanDH project. It addresses the processing of data of project partners as well as external participants and contributors.
Present the main methodological approaches in bullet point format	
What were the main findings or take-away messages? What implications does it have for the XpanDH project?	
Which project stakeholder group would benefit the most from the document and why?	

Healthcare Professional	
International Adherence Network/Initiative	
Investors and Funding	yes
Patient Organization	
Patient/Caregiver	
Pharma (Marketing & Sales / Medical Dept./ R&D)	
Public Authority or Policymaker	
Regulatory body	
Standardization Body/ Open-Source Network Researcher/Academic	
Statutory Health Insurance Company	
Technology & Service Provider	
Other	

List any relevant organizations or social media accounts for wider visibility	

Revision History			
Version	**Date**	**Author**	**Description**
0.1	01/10/2024	Anderson Carmo	1st document outline (based on D1.6)
0.2	29/11/2024	Petra Wilson	1st full draft
0.3	05/12/2024	Henrique Martins	First Review
0.4	20/12/2024	Anderson Carmo	Updated of the deliverable content accordingly the comments received.
1.0	30/12/2024	Anderson Carmo	Final revision on the document prior EC submission.

Table of Contents

List of abbreviations

Acronym	Description
EEHRxF	Electronic Health Records Exchange format
FAIR	Findable, Accessible, Interoperable, Re-usable
GDPR	General Data Protection Regulation
REC	Research Ethics Committee

Executive summary

This document sets out the Data Management Plan for the XpanDH project. XpanDH is a Coordination and Support Action that aims at mobilizing and building capacity in individuals and organisations to create, adapt and explore purposeful use of interoperable digital health solutions based on a shared adoption of the European Electronic Health Records Exchange format (EEHRxF) across Europe.

The Data Management Plan is divided into two main sections. Following an introduction section two sets out the legal requirements of **processing of personal data** in accordance with the General Data Protection Regulation (Regulation (EU)2016/679)[1]. The third section sets out the requirements to be met to ensure that data generated by the project may be lawfully re-used by other are researchers **Findable, Accessible, Interoperable and Re-usable (FAIR**) as required Horizon Europe Data Management Plan guidance.

The section on **Processing Personal Data** is divided into three parts. It looks first at the legal and ethical requirements of processing of personal data of project partners in the context of project work. It then considers the legal and ethical requirements of processing of personal data collected in the context of the project from people who engage with the project at webinars, events and through newsletters and similar tools, but who are not signatories to the Grant Agreement and therefore have no contractual relationship with the project consortium. Finally, this section looks at the legal and ethical aspect of collecting and processing sensitive personal data, such as health related data. This has only limited relevance to XpanDH, but is included for completeness.

Section three, under the heading of **Ethical and FAIR data processing** considers briefly requirements of processing data in the context of any experimentation and testing and ensuring they can be re-used where appropriate. This is set out according to the Horizon Europe Data Management Plan Template.

This Data Management Plan is a live document, it will be updated as needed and as the data processing activities of the project partners become clearer. It is designed to support both the project centrally, as well as individual partners in their data processing activities.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

1. Introduction

1.1. Background

XpanDH is a Coordination and Support Action designed to build capacity in individuals and organisations to be ready to use the European Electronic Health Records Exchange Format (EEHRxF). It seeks to create, adapt, and explore purposeful use of interoperable digital health solutions through an EEHRxF Network of Networks. The Network is built up among stakeholder and experts in the field and seeks to support them with tailored guidance and real examples to help them advance in the use of EEHRxF-embedded digital health solutions. Its overall objective is to ensure that using EEHRxF based solutions adds value to health and care and promote Personal and European Health Data Spaces.

A key aspect of this is to build X-bundles, which are an aggregation of interoperability assets that support the connections and interconnectivity between health systems based on the specifications of the EEHRxF. The X-Bundles are developed through X-Bubbles, which bring together key stakeholders from across the healthcare continuum and across EU Member States experiment with using the EEHRxF.

As part of this work the project partners must work together, thereby exchanging personal and non-personal information. The ideas and concepts they develop will be shared and tested with healthcare system stakeholders outside the project to gather input and experience, therefore again collecting and processing personal and non-personal data. And finally, to be successful in meeting the objective of increasing uptake of the EEHRxF-embedded digital health solutions, the project partners will engage in a wide range of outreach activities which will include webinars, meetings, conferences and dissemination of newsletters, which will require the data of participants and recipients to be collected.

Although the XpanDH project is concerned with developing and testing interoperability solutions, all testing will be done either with dummy data or will be done in the context of the everyday work of partners. Where trials are done in the context of everyday work any real patient data that may be involved will be under the auspices of the organisation engaging in any form of trial. It will fall outside the project, any data reported from such partners into the project will be fully anonymised.

From a data governance perspective therefore, the project has minimal demands, which are limited to ensuring that the personal information of project partners are processed in accordance with their reasonable expectation under the terms of the Grant Agreement; and that personal data are collected from individuals who are not party to the Grant Agreement are processed lawfully, as set out below.

1.2. Scope and objectives

The scope and objective of the Data Management Plan is to address the legal and ethical requirements of the project. It has been prepared to enable appropriate interpretation and application of ethical and data protection principles throughout the project's life cycle and beyond.

The Data Management Plan addresses four elements falling into two broad categories: **processing of personal data in accordance with the legal requirements of the General Data Protection Regulation** (Regulation (EU)2016/679) ; and **Ensuring that data generated by the project that may be lawfully used by other are Findable, Accessible, Interoperable and Re-usable (FAIR)** as required by the Horizon Europe Data Management Plan guidance.

This Data Management Plan is a live document, it will be updated as needed and as the data processing activities of the project partners become clearer. It is designed to support both the project centrally, as well as individual partners in their data processing activities. Where data are collected and stored by a project partner, each partner is legally responsible for compliance with data protection legislation in the country in which the organisation is legally established. Where data are processed by the project co-ordinator for the project as a whole, the legal responsibility for its appropriate processing and storage is with Iscte-CVTT in Lisbon. Any data of the project stored for longer term use will be in Zenodo.

2. Processing of Personal Data

In the context of the project personal data are generated from two types of sources: the project consortium in the context of the partners work on the project, and personal data collected in the context of the project from people who engage with the project at webinars, events and through newsletters and similar tools, but are not member of the consortium.

Data generated from both types of source must be processed in accordance with requirements of the General Data Protection Regulation (Regulation (EU)2016/679), generally known as the GDPR. However, the legal basis on which they may be processed will not be the same.

In the first group the relationship between the partners is based on a contract to which they are all party, the Grant Agreement, data are therefore processed on the basis of fulfilling the obligations under the contract and do not require any further consent or explanation. However, only data relevant to the execution of the contract may be collected and processed. In the second group no contractual relationship exists between the parties, so another legal basis must be established. This will usually be consent. The concept of legal bases for data processing comes from the GDPR which is outlined below.

The GDPR was enacted in 2016, building on the previous Data Protection Directive of 1995. The new law is a Regulation, not a Directive, meaning that it is directly applicable in every Member State and does not have to be transposed into national legislation.

2.1. General Data Protection Regulation (GDPR)

The GDPR creates duties for data controllers and gives rights to data subjects. **Deliverable 1.5.2 on the Legal Framework of Digital Health** gives a thorough explanation of the GDPR, a short summary is provided in the table below, showing how the key requirements impact XpanDH

Figure 1 : GDPR in XpanDH

GDPR	Summary	Impact on XpanDH
Scope and Applicability	The GDPR applies to all organizations that process personal data of individuals within the EU, regardless of the organization's location. It also applies to organizations outside the EU that offer goods or services to people in the EU. It applies to personal identifiable data. Special rules apply to sensitive personal data, such as health data.	Applies to all the organisations that are partners in XpanDH and applies to the individual behaviour of the people working in the project, although liability for their behaviour will apply to the organisations that are their legal employers,
Rights of Individuals:	The GDPR grants individuals rights regarding their personal data. These rights include the right to access their data, rectify inaccurate information, erase data (the "right to be forgotten"), restrict processing, data portability, and object to processing for certain purposes.	XpanDH partners must be able to provide access to data if they have collected it, and to portability of such data if it was collected on the basis of consent.
Duties of Data Controllers:	The legal and natural persons who are responsible for how data are processed (whether by themselves or an entity or person employed by them to	Each XpanDH partner must know who is responsible for compliance with GDPR in their organisation and

	process data on their behalf) are data controllers. They have to ensure that they can meet the rights of the individuals whose data they process and that they have a legal right to process that data. If a data breach occurs, the data controller must notify this to the national authority and data subjects.	ensure they have the approval of the responsible person to process data. Data must be stored securely.
Legal Bases for data processing:	The legal bases available are: • Consent • Contractual necessity • Legal obligation • Vital interests • Public tasks • Legitimate interest When the data are sensitive data, such as health data, a further legal basis must exist, this must be one of the following: • Explicit consent • Legal obligation • Vital interests • Legitimate interest • Data made public by data subject • Legal claims • Public interest • Healthcare • Public health • Public interest Legal basis for processing data int the context of healthcare is usually based on the legal obligation of the data controller (a healthcare provider, to collect data in order to treat a patient properly. .	In XpanDH if data are collected from project partners or from event participants. For project partners' data the legal basis is likely to be the contractual relationship between the partners based on the Grant Agreement. For data from people outside the project attending events and other connections, consent is likely to be necessary. This requires that an information notice must be provided that tells data subject detailing what data will be collected, for what purpose and how long it will be kept (inter alia). It is unlikely that the project will process any sensitive data collected specifically for the project at project level. If such data are collected in the routine work of project partners and re-used in

		the project, the data will be anonymised and will fall outside the GDPR.
Data Transfer	Restrictions on transferring personal data outside the EU to countries that do not provide an adequate level of data protection. Organizations can use various mechanisms, such as standard contractual clauses or binding corporate rules, to ensure adequate safeguards for such transfers.	Any person identifiable data XpanDH partners collect should not be sent outside the EU

The table above provides a summarised overview of GDPR, some of the implications on the project will be discussed in more detail in the sections below.

2.2. Processing project partners' personal data

The conduct of a project necessarily entails the generation of a great deal of data about the consortium partners and the work they conduct. The consortium partners have a duty towards each other to ensure that such communications and data are treated respectfully, and in compliance with GDPR.

In terms of GDPR compliance the legal basis lies in the contractual relationship between the partners. This means however that the data collected relate to the execution of the contract, it cannot be used to justify collection of data that are not needed for completing the work of the project.

The data collected will generally include personal data when work tasks are reported, notably within time reporting, but it also includes significant amount of email traffic, report drafting and other creation of data trails. It will involve collection of personal data from consortium members during virtual meetings conducted over Teams or other platforms., e.g., recordings, pictures or field notes. This means the following data will be recorded about project partners:

- name and registration details provided
- image, if a camera is used at any time during virtual meetings
- voice, if a question is asked or comments are made orally
- any text provided in a chat function.

The project communication operates on the basis of Microsoft Teams and Microsoft SharePoint and email communication. All reports, deliverables, minutes and other text-based material is stored within the Microsoft Teams environment and hosted on the secure servers of ISTCE at the University of Lisbon which operates the log-in process for access to the Teams site. Microsoft Teams is built on the Microsoft 365

and Office 365 hyper-scale, enterprise-grade cloud, delivering advanced security and compliance capabilities**.** The data controller for this type of information is ISTCE who undertakes to keep such data safe. Long term security storage is made on Zenodo[2].

2.3. Processing non-project partners personal data

A key focus of the XpanDH project is building capacity and engagement on the use of the EEHRxF. This involves consortium partners working with external partners who will typically provide the project with their names, affiliation, contact details, and may also share professional background data as well as their experiences and opinions.

Where personal data from participants are collected, these data are collected on the basis of informed consent, are used only for the purposes states (usual to provide further project related information) and are stored in a specifically designated folder with access restricted solely to the team directly involved in XpanDH management.

Where the engagement with external parties is more active, for example through surveys or other formats where people may provide personal data other than name and contact details, all data collection will again be based on informed consent. All interviewees, focus group participants and other external parties will participate voluntarily. The personal data will be processed under the regulations of GDPR and national legislations of partner countries where events take place. The request for consent will be presented in a manner that is in an intelligible and easily accessible form, using clear and plain native languages of the participants.
In the case of a personal data breach, the controller will without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the national supervisory authority. Where the notification to the supervisory authority is not made within 72 hours, it will be accompanied by reasons for the delay. The processor will notify the controller without undue delay after becoming aware of a person data breach.

2.3 Processing sensitive personal data

The GDPR classifies some data as sensitive personal data. This data which reveals any of the following:

- Racial or Ethnic Origin
- Political Opinions
- Religious or Philosophical Beliefs
- Trade Union Membership

[2] https://zenodo.org/communities/xpandh/records?q=&l=list&p=1&s=10&sort=newest

- Biometric Data:
- Sex Life or Sexual Orientation
- **Genetic Data: Data concerning the inherited or acquired genetic characteristics of an individual, which can be derived from analysis of their biological samples**.
- **Health Data: Data that pertains to an individual's physical or mental health, including medical conditions, treatments, and health services received.**

Processing of sensitive personal data is generally prohibited under the GDPR unless certain conditions or exceptions apply. However, there are specific circumstances where the processing of such data is allowed, such as explicit consent from the data subject, obligations related to employment or social security, **processing for the provision of healthcare,** as well as the other legal bases set out in the table above.

2.3.1 Sensitive personal data in XpanDH

It is not anticipated that any sensitive personal data will be collected for the purposes of the tasks in XpanDH. At this stage therefore, no ethical review process for collecting sensitive personal data from any trial participants or patients. Although it is possible that in the context of taking part in trials or experiments project partners involved in the X-Bubbles may use some patient data, this will be done under the auspices of their everyday work. Any such data collection and processing will take place outside the project remit and will be conducted under the supervision and approval of the data protection office of the relevant project partner. Should any information be provided to the project it will be fully anonymised. As anonymised data are not covered by the GDPR there are no further EU level legal requirements to address. However, national level legislation may exist which must be addressed by the relevant project partner.

If at a later stage in the project it becomes clear that sensitive data will be collected and used within the remit of the project, the relevant ethical and legal procedure will be set up. This will include the provision of a template for a privacy information notice and support in obtaining ethical compliance from a Research Ethics Committee or other relevant approval body.

3. FAIR data

3.1 Making data findable

The project will not create significant amount of primary data. Results from surveys or focus groups will be available in public deliverables.

In order to make the XpanDH bundles FAIR the project will develop data tags to support data integration, analysis, storage and sharing. If appropriate tools such as

data dictionaries may be designed and developed during the project to make data from the project more findable.

A naming convention has been adopted for documents that includes a standardised naming format for all documents and datasets and a series of Unique Identifiers: ensuring that each document and or data set is referenced by a unique identifier to ensure effective version control. For open data repositories, DOI will be used as the standard unique identifier in line with ISO 26324.

3.2 Making data accessible

The consortium is committed to making results and data from the project available at the appropriate time-points and has included provision for open access publications within the budget for this purpose.

3.3 Making data interoperable

A core objective of the project is to promote interoperability solutions for digital health. Accordingly, the project will be focussed also on ensure that the information it generates is interoperable across different actors and stakeholders.

3.4 Increase data re-use

The projects' overall commitment to interoperability and FAIR data will ensure that the data models, labels, nomenclatures and conventions developed in XpanDH support the re-use of XpanDH Bundles and data where this may be done in accordance with GDPR and other applicable legislation.

4. Intellectual Property Rights

The lawful use intellectual property either brought to the project by partners (background IP) or generated by the project (foreground IP) is detailed in the Project Consortium Agreement. Annex 1 of the Consortium Agreement details all the Background information brought by each partner.