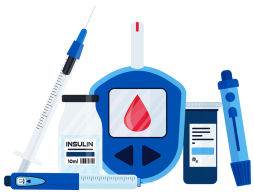

DigiCare4You

DIGICARE4YOU DATA MANAGEMENT PLAN (DMP)

DigiCare4You aims to improve the early prevention and management of Type 2 Diabetes (T2D) and hypertension (HTN) via a community-based, person-centered solution, integrating both social and healthcare systems, supported by the use of digital tools.

DigiCare4You is a research project that is collecting and producing large sets of data. A Data Management Plan (DMP) has therefore been developed to comply with legal and ethical requirements concerning data processing. The DMP outlines how data will be processed and handled during, and after completion of, the DigiCare4You project. It also includes an overview of the datasets that will be produced by the consortium partners and the rules that should be followed for data processing. In addition, it provides an outline of the measures taken to comply with ethics and data protection and data security.

PURPOSE OF THE DMP

Research has many phases, from planning and collecting to processing and analysing data. The DMP provides principles and rules for conducting the various research steps to satisfy processing and protection requirements. For example, it provides insights on what data will be generated, how it will be exploited and how it will be made accessible, reusable and be stored during the project and after its completion. The DMP also provides a strategy for managing data and is a source of formal self-regulation that outlines how the data will be handled during the project. Finally, it shows the commitment of the DigiCare4You project towards upholding the highest standards of research integrity in compliance with, and with respect to, the ethical standards of national and international legislations and rules of Horizon programs.

DATASETS IN DIGICARE4YOU

DigiCare4You's data sets include structured and unstructured data, quantitative and qualitative data as well as text and numerical data. An overview of the data that consortium partners will collect or generate, including owners, purpose, accessibility level, type and format, as well as information about data origins and re-use of existing data, can be found in the DMP.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 945246

THE FAIR REQUIREMENTS

DigiCare4You will be following the European Commission recommendations of the FAIR requirements, meaning that research data should be findable, accessible, interoperable, and reusable. To showcase how the FAIR principles will be followed during the project, a detailed set of instructions for partners has been outlined within the DMP. This includes, for example, how data will be made findable internally and externally from consortium partners, how project results should be made accessible to the public, how partners will make their data interoperable through the consistent use of common, standardised file formats, and how consortium partners will make data produced in this project possible to reuse.

F INDABLE
A CCESSIBLE
I NTEROPERABLE
R EUSABLE

ETHICS AND DATA PROTECTION

Beyond the FAIR principles, the DMP details how potential ethical issues in data processing should be managed according to ethical standards and regulatory provisions. The DigiCare4You project underwent ethics evaluation, resulting in conditional ethics clearance. The conditional ethics clearance means that the project can run as long as ethics requirements are met. The ethics requirements were grouped under the three categories of 'humans', 'protection of personal data' and 'other issues'. These requirements are important for the handling and processing of data within the project and are therefore outlined along with the solutions that consortium partners will implement. This is outlined further in deliverable 3.1.

DATA SECURITY

The final section of the DMP outlines the data security measures undertaken by consortium partners. Notwithstanding the lack of uniform implementation of security measures by project partners, it was stipulated that each partner accesses the appropriateness of the security measures taking into account relevant factors as laid down by the GDPR. Therefore, some of the data security that are recommended include:

- The storing of data in a password-protected repository;
- The establishment of additional security procedures to preserve data by carrying out regular back-ups of folders and information stored;
- The adherence to good security practices by protecting devices and installing and updating anti-malware software, anti-virus software and enabling firewalls;
- The use of proper anonymisation techniques to ensure the preservation of personal privacy and the protection of personal data;
- The notification of any potential data breach within 72 hour after partners becoming aware of it;
- The documentation of any personal data breaches, their effects and remedial actions taken.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 945246