TransCare

New care pathways for supporting TRANSitional CARE from hospitals to home using AI and personalized digital assistance

D3.3 – Ethical standards and data management plan

Related Work Package:	WP3
Related task(s):	T3.3
Related milestone:	Mil 1
Version:	1.0
Status:	Final Version
Dissemination level:	PU
Deliverable type:	R
Due date of deliverable:	M12 (April 2025)
Actual submission date:	29 April 2025
Deliverable lead partner:	KRD
Main author(s):	Riitta Hellman (KRD), Terje Grimstad (KRD)
Contributing authors:	Lars Thomas Boye (TLU), Ionut Anghel (TUC), Camilla Gabrielsen (FAR), Ancuta Nemes (HINS)
Peer-reviewers:	FAR and TLU
Keywords:	Project ethics, data management plan

Project partially funded by European Union and Unitatea Executiva pentru Finantarea Invatamantului Superior, a Cercetarii, Dezvoltarii si Inovarii (UEFISCDI) (RO), The Research Council of Norway (NO), and Italian Ministry of Health (IT).

Version history

Version	Authors	Date	Description
0.1	KRD (R. Hellman)	05.03.2025	First content structure
0.2	KRD (R. Hellman)	07.04.2025	Content draft, 1st version
0.3	TUC (Ionut Anghel)	08.04.2025	Added Ch 5, individual data management plans and TUC plan
0.31	KRD (Erlend Øverby)	11.04.2025	Updated 5.3, KRD plan
0.32	TLU (Lars Thomas Boye)	11.04.2025	TLU data management plan
0.33	HINS (Ancuta Nemes)	11.04.2025	HINS data management plan
0.34	FAR (Camilla Gabrielsen)	14.4.2025	FAR data management plan
0.5	TUC (Ionut Anghel)	15.4.2025	Different fixes and inputs added
0.9	KRD (Terje Grimstad)	15.4.2025	Review ready version
0.95	TLU (Lars Thomas Boye) FAR (Camilla Gabrielsen)	28.04.2025	Peer-review
1.0	TUC (Ionut Anghel)	29.04.2025	Final version

Contents

List of acronyms

Acronym	Description
EU	European Union
FAR	Farsund kommune (Farsund Municipality)
GP	General Practitioner
HINS	The Heart Institute Niculae Stăncioiu
INRCA	ISTITUTO NAZIONALE DI RICOVERO E CURA PER ANZIANI
KRD	Karde AS
ML	Machine Learning
RPM	Remote Patient Monitoring
THCS	Transforming Health and Care Systems
TLU	Tellu AS
TUC	Technical University of Cluj-Napoca
WP	Work Package

Executive summary

In this deliverable, the TransCare consortium presents the ethical guidelines to be applied in the project. These guidelines cover (a) the European rules and regulations that follow from the AAL programme and from the European legislation for research ethics, privacy, and data protection, and (b) the national guidelines that the partners are obliged to follow according to national rules and regulations.

In this deliverable, the ethical principles that were drafted in the project Description of Work (DoW) are systematised and presented.

The data management plans (DMP) of the consortium and all partners are also presented. These plans cover both the end user partners' plans and those of the technical partners; all types of project partners have certain aspects of data management that must be considered along the project's lifetime. The DMPs are detailed according to the THCS programme's DMP template.

1 Introduction

This document is the second deliverable from Work Package no. 3: 'Transitional Care Knowledge Building and Care Pathways Design' (duration M1-M36, total effort 37 person months).

Table 1: Description of task 3.3

Participant nº	1 (coord)	2	3 (task lead)	4	5	6 (WP3 lead)
Participant short name	TUC	TLU	KRD	INRCA	HINS	FAR
Participating in Task 3.3	0	2	6	3	0	3
Task 3.3 Ethical standards and data management plan Ethical standards, in terms of fair treatment of participants, respect of human rights, accountability in research, data protection and security, anonymity, etc. will be taken under careful consideration to ensure compliance with European legislation and criteria. Ethical and legal rules and regulations will be horizontally applied in all work packages, as required by the framework of Ethics by Design, Ethics by Context, and Ethics by Individual. The consortium will apply best practices in data protection and privacy including advanced protection. Crucial disclaimers will be implemented in the final system operation. The ethical management activities will continue until the end of the trial's activities.						

2 The pilot sites

The TransCare project has three pilot sites: one in Italy (INRCA), one in Norway (FAR) and one in Romania (HINS). The ethical standards of the project are particularly important for the pilot sites and the conduct of the project pilots, and the application of the technologies resulted in the project.

2.1 FAR

Farsund municipality operates as a comprehensive healthcare organization, offering a range of services to support rehabilitation and independent living. In the FAR pilot, a digital short-term unit will be integrated into the municipal care services. While telehealth is already a part of their regular municipal services, the aim is to provide patients with a safe and flexible transition from hospital to home, with close follow-up. The TransCare project seeks to reduce readmissions and offer care comparable to a physical short-term care unit. The objective is to support the transition of these patients to receive care at home by implementing specific municipality health services using the technology developed in TransCare, along with other welfare technologies provided by TLU. The welfare technologies already in place in the municipality in the TLU platform include safety alarms, cameras, movement sensors, and GPS, among others, and will only be used it the Norwegian pilot.

2.2 HINS

The Heart Institute Niculae Stăncioiu (HINS) is one of the most important tertiary cardiology centres in Romania. Complex cardiovascular diseases are diagnosed and treated in patients of all age groups, ranging from children with congenital heart diseases to elderly patients with valvular heart disease or heart failure using various interventional and surgical approaches. It is also a medical research centre for cardiovascular pathology. The institute receives patients both as inpatients and outpatients. The cardiology department provides 24-hour service for patients suffering from angina, myocardial infarction and other acute cardiovascular conditions. Monitoring is an important part of cardiovascular diseases management in all stages of primary or secondary prevention by optimising the control of risk factors, early identification of patients at higher risk of readmission that may allow for targeted interventions to reduce the readmission rate. In the HINS pilot, they will play a key role in evaluating and refining transitional care practices for cardiovascular diseases. They work closely with other healthcare providers from the region to ensure seamless integration and effective delivery of transitional care services.

2.3 INRCA

Istituto Nazionale di Ricovero e Cura per Anziani Italy (IRCCS-INRCA) is a geriatric clinical and research hospital, and it is the leader of Italian Ageing Network. The INRCA pilot will play an important role in transitional care by providing support and services to individuals who are transitioning from one healthcare setting to another, bridging the gap between acute care and long-term care or home-based care. Typically, the patient who will be involved is a multimorbid older adult admitted within the Geriatrics operating unit. The clinical scenario is usually multimorbid with previous chronic diseases often different from the one for which they are hospitalized. The transition from the hospital setting to home is therefore a leading and challenging issue for the institute and certainly crucial in improving the quality of post-hospital intervention in terms of personal care and support. The role of INRCA within the pilot is to identify a population at risk of rehospitalisation by defining inclusion and exclusion criteria.

3 The ethical foundation of the TransCare project

The ethical requirements of the TransCare project stem from the fundamental goal definition of the TransCare project: The main goal of this project is to address the open challenges and necessities previously identified for the health and care systems by adapting, scaling, and evaluating a technology-assisted transitional care solution based on IoT monitoring, ML, and digital assistance to a larger number of patients and considering the specific contexts of different healthcare systems in Europe (NO, IT, RO) as well as various types of comorbidities.

To administer the ethical considerations and the project practice, the principles and guidelines presented in this chapter will be carefully followed in all phases of the project.

3.1 TransCare main ethical cornerstones

The ethical awareness, as well as the TransCare project practices, will be based on the AAL Guidelines [1]. Also, the project will follow EU and national requirements, recommendations and guidelines in ethics, privacy, and information security.

The use of the TransCare platform poses several ethical concerns that will be carefully addressed in project implementation ethics by design, context and individual [2]. Participation in research is yet another issue of ethical concerns. Some are directly related to the characteristics of the technologies involved, some to issues of preferences and choices. In all matters concerning the contact with and involvement of patients and their formal and informal caregivers, ethics and information security will be strongly in focus.

Ethical issues will be handled by five concrete approaches in the TransCare project:

1. Applying the project's daily ethical guidelines to be followed by all researchers and practitioners participating in the project.
2. Applying for ethical approvals from national ethics boards and committees, per each participating country's research ethical regime, appropriate and necessary for the project's topic.
3. Making all necessary self-declarations and the like, in each participating country vis-a-vis national rules and regulations for data security arrangements and that of handling person (-al)/sensitive data, and privacy.
4. Following relevant EU and national laws, data acts, and directives.
5. Embedding organisational structures and procedures in the project for ethics management.

The project's daily ethical guidelines will address the following issues of special relevance, and are to be kept in mind of the researchers as well as the practitioners:

- The recruitment process will be carried out based on defined eligibility criteria for participants conforming to the ethical procedures.
- Information: Any information, requests, and interaction with the (potential) participants will be presented with respect, and in a way that the participant can understand.
- Willingness and ability to participate: The TransCare project will bear in any dependencies or other relations between any parties that might influence the end-users' feeling of willingness to participate (interviews, field studies, and user tests, pilots etc.), or cognitive and physical ability.

- Principle of informed consent to elicit and store data – freely given, specific, and informed.
- Participants must be allowed to exit any project stage (such as focus group, experiment, test, or trial) at any time, without any obligation to explain their reasons.
- Trust and comfort are key issues in home care. Possible conflicts or stressful relations between primary and secondary end-users (e.g., caregivers requiring monitoring/tracking, and the primary end-user refusing to be monitored) will not offer a fruitful or ethically acceptable point of departure for any test, trial, or pilot.
- Clarification of who is to be the responsible organisation and what is the purpose of any data collection, especially who is the controller and processor of any personal data.

3.1.1 Informed consent

The consortium will produce a detailed informed consent process that will include information such as:

- the purpose of the procedures
- the foreseeable risks and discomforts of the end-user
- the benefits to the user
- the confidentiality of data records
- whom to contact for answers, etc.

The informed consent will be signed by each participant of the user involvement or, in the case of cognitive impairment by the person authorised to do so. It will contain a clause informing the user that he or she can quit cooperation at any time without any negative consequences. None of the project activities involving end-user participants constitute clinical research or medical intervention. Nevertheless, if required, the appropriate national Ethics Committees will be contacted before starting any activities related to these studies. User tests and pilots will reveal the most important parameters concerning dignity. In all cases of fieldwork, the dignity and autonomy of participants will be upheld. By dignity, we mean the personal experience of confidentiality and personal comfort when using or being monitored by ICT or communicating with it. One part of the personal comfort is to use non-intrusive technology solutions, such as small sensors if these are wearable ones, not monitoring the private life through web cameras at all times of day, etc.

3.1.2 Privacy, integrity and comfort

One very important issue is that the privacy, integrity, and comfort of the patients are respected. Personal data will be collected and processed according to the provisions of the partners' national legislation, fulfilling the General Data Protection Regulation (GDPR) (EU) 2016/679 [1], which is a regulation in EU law on data protection and privacy for all individuals within the EU. The challenge in data privacy is to collect and analyse necessary data while protecting personal and identifiable information. The consortium will apply best practices in data protection and privacy including providing advanced protection through data security, authentication processes, and encrypted data. Moreover, the data will be fairly and lawfully processed, processed for limited purposes, adequate, relevant, and not excessive, accurate, not kept longer than necessary, processed following the person’s rights, secure, and not transferred without adequate protection. When required, approvals for the collection and processing of personal data by the National Data Protection authorities will be acquired. These data will be processed and analysed requiring authorisation by the end-user and/or caregivers.

3.1.3 Safeguarding data confidentiality

The overriding priority will be to safeguard the patient's confidentiality and to ensure clearly defined processes for different uses of their involvement. TransCare will ensure that no identifiable information is made available without explicit consent. After that the consent has been obtained for the use of personal information, the use of that information, storage, access, and length of storage will form part of the information given to pilot participants before consent. Our approach to confidentiality is to protect the patients' information by building appropriate access rights, encryption, anonymisation, and provenance techniques into the core models of the TransCare platform. During piloting, all personnel involved including system evaluators, service providers, etc., sign a confidentiality agreement to maintain the privacy of involved employees and their information. Where necessary, their information will be anonymised.

3.1.4 Ethics procedure for the end-users leaving the pilot

In cases where patients choose to withdraw from or leave during a pilot, the following will apply:

- The patients' collected personal information will be discarded and destroyed.
- System or devices installed at their site, if any, will be uninstalled and dismantled and their accommodation will be restored to the same state as before the installations.
- Patients who stay until the end of the pilot or end of the project, their personal information will be deleted by the project completion and/or as specified in the consent form. Equally, they may choose to keep system installations that are available for continued use or get them dismantled (if any).

The Legal, ethical, and security group of the project will ensure that all necessary local ethical approvals are obtained. Furthermore, they will provide advice and observe the ethical practices concerning the relationship between all end-user groups and the project, including formal and informal caregivers.

In particular, the TransCare pilots will be evaluated in three different test sites (FAR, HINS, INRCA). During these, a proof-of-concept study methodology will be used to explore the impact and validity of the second and complete prototype. Ethics, usability, acceptance, and generally, several functional and non-functional system characteristics will be assessed by standardised instruments (questionnaires).

3.1.5 Opt-out, exit strategies and drop-out management

All end-users will be informed about their right to exit the project at any time during the ongoing pilots. They can be asked for the reason for exit, but it will be made clear that there is no obligation to answer. End-users will be interviewed about TransCare concerning its effectiveness, perceived usefulness, and user-friendliness but also about what kind of problems might arise, or which factors affect negatively the users' willingness to use the envisioned technology. Partners are aware of the high drop-out rates in research studies and have already provided for proactive (inclusion of a larger cohort of end-users than sufficient) and reactive strategies (maximisation of recruitment efforts) to mitigate the risks.

Further, people might become dependent on using TransCare technology. Therefore, the consortium will make sure that the patients can continue using suitable and available parts of the TransCare

system after the project end. Alternatively, the consortium will help the patients to find an alternative solution.

The TransCare exit strategy will be adaptively applied when end-users leave the project during implementation or concluding phases to ensure that they do not feel abandoned or lost due to the withdrawal of attention, technology, etc. We will analyse the situation of each end-user involved to detect if some individuals developed a strong dependency, and what possible problems might arise to make the transition as comfortable as possible.

End-users who wish to continue using TransCare after the project end, may be given the option to keep and continue to use them (depending on the cost and financing) or will be guided to an alternative solution for cognitive state self-management. At the end of the project, patients that require help for re-adapting will be provided with information about alternative help organisations, entities, and web sites that provide support for (self) care management. Also, they will be informed when the project results and solutions are available on the market.

3.2 Ethical impact

Ethical impact is another aspect of ethics than those which concern privacy aspects and such. For the patients the TransCare system provides the following ethical impacts:

- Promotion of autonomy, dignity, and self-confidence through the rehabilitation period.
- Enhancement of their ICT literacy and self-confidence: Technology is adapted to them in contrast with them adapting to technology.
- Opportunity to preserve dignity and self-management of health at the patient's own home.
- Better remote monitoring for remote patients (telehealth services).
- Informal caregivers receive options to obtain care supporting wellbeing information from the patient.
- Informal caregivers may experience relief of care burden.
- Therapists receive options to obtain therapy supporting wellbeing information from the patient.
- Right for healthy adults to authorise who views their data.

According to our ethical plan, all ICT features if TransCare provided will ensure the privacy and protection of personal data according to common protocols.

3.3 Ethics management organisation

The national (local) ethics managers will monitor project ethics in the countries in which pilots will take place, making sure that the local regulations are respected. In particular, is responsible for:

- Applying for ethical approvals from national ethics boards and committees, according to each participating country's research ethical regime, appropriate and necessary for the project's topic.
- Making all necessary self-declarations and the like, in each participating country vis-a-vis national rules and regulations for data security arrangements and that of handling person (-al)/sensitive data, and privacy.

A Legal, Ethical and Security Group will be comprised of all the National (Local) Ethics Managers and will work to ensure that all EU level ethics are respected and to harmonise potential local (national) ethics-related differences.

The committee, presented in Table 2, will:

1. Define the project's daily ethical guidelines to be followed by all researchers and practitioners participating in the project.
2. Ensure that researchers' interactions with end-users are ethical and best practices ethical management has been applied.

Table 2: Legal, Ethical and Security Group

Country	Name	Participant
Italy	Dr. Roberta Bevilaqua	INRCA
Norway	Dr. Riitta Hellman	KRD
Romania	Dr. Ovidiu Anchidin	HINS

3.4 European ethical guidelines

3.4.1 EU and national laws, data acts, and directives

The TransCare project will comply with all national and European regulations and legislations to guarantee adherence to ethical standards and will have a significant impact on users' lives ethically and socially. Most important is to fulfil the General Data Protection Regulation (GDPR) (EU) 2016/679 [1], which is a regulation in EU law on data protection and privacy for all individuals within the EU.

3.4.2 AAL guidelines

For WP3, the DoW requires ethics by individual to be implemented in each task [2]. Examples that illustrate these requirements are [2]:

- behaviour and awareness
- aspects that chat can be improved for the end users
- learning how to use the technology
- communication about the (effects of) the new technology
- combatting digital literacy and digital divide
- health professionals training to use the new product/service

In the TransCare project, ethics by individual will be implemented in the communication with end users about the TransCare technology itself. This strategy leans on two main perspectives:

- to ensure that the AAL values (Figure 1) ere embedded in the communication with end-users in all categories
- to ensure that aspects such as those in the bullet list above, are well present when implementing and evaluating ethics in the TransCare project

Implementing and monitoring ethics is a shared task between all WP-leaders, the Legal, ethical and security group, and the task leader of Task 3.3.

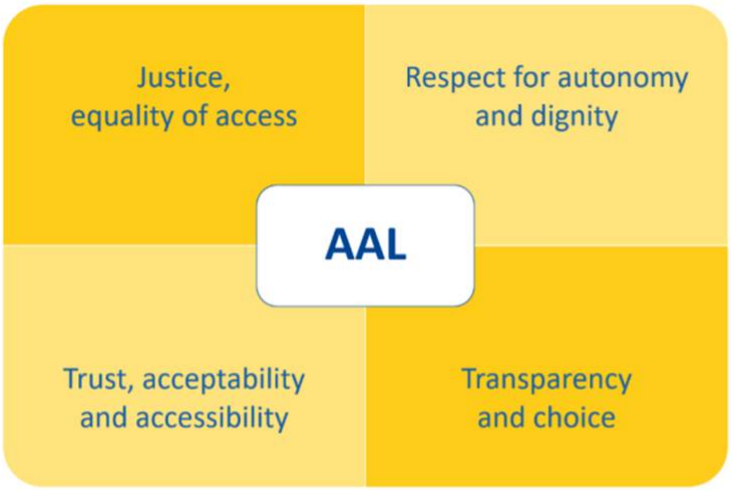

Figure 1: The AAL ethical values.

The implementation of ethical principles [2] in the work packages of TransCare is fully covered in the in the project. This is illustrated in Table 3.

Table 3: Implementation of the AAL ethical principles in the DoW.

Ethics principle	WP1	WP2	WP3	WP4	WP5
Ethics by design	x		x		x
Ethics by context	x	x	x	x	
Ethics by individual	x		x		

4 Pilot-specific ethical approvals

4.1 FAR

In Norway, the Norwegian National Research Ethics Committees have established 'General guidelines for research ethics. The four main principles are [2]:

Respect. People who participate in research, as informants or otherwise, shall be treated with respect.

Good consequences. Researchers shall seek to ensure that their activities produce good consequences and that any adverse consequences are within the limits of acceptability.

Fairness. All research projects shall be designed and implemented fairly.

Integrity. Researchers shall comply with recognised norms and to behave responsibly, openly and honestly towards their colleagues and the public.

These guidelines supplement the research ethical guidelines for the Norwegian partners, in addition to the daily ethical guidelines and AAL ethical requirements, in the TransCare project.

In Norway, the TransCare project sorts principally under REK, the National Committee for Medical and Health Research Ethics.

National Research Ethics Committees secretariat was contacted for first evaluation (detailed documentation of the project was attached). The first evaluation documented the rules and the steps to make a self-evaluation of the need to apply for a formal approval. The self-evaluation of the TransCare project shows that it is not relevant to apply for ethical approval in REK. The MDR or DMP criteria (development of medical devices or products) is not fulfilled. For the purposes of the TransCare project, we do not have to apply for an ethical approval. This has been fully clarified by the correspondence between REK and Dr. R. Hellman in KRD. This clarification will also apply for the pilots of TransCare technologies from KRD and TLU.

Karde's WP3 leader, Dr. Riitta Hellman, has by The Norwegian Data Protection Authority been registered to be Karde's privacy ombud. She has the competency and capacity to monitor and supervise all ethical aspects connected to the TransCare project's Norwegian part.

4.2 HINS

The research studies within the TransCare project were approved by the ethics board of the hospital under request no. 4678 dated April 11, 2024. Upon completion of the final protocol, the study will be presented to the local ethics committee.

4.3 INRCA

Ethics committees are independent bodies responsible for ensuring the protection of the rights, safety and well-being of trial subjects and for providing public assurance of that protection. Where not already assigned to specific bodies, ethics committees may also perform advisory functions in relation to ethical issues connected with scientific and care activities, with the aim of protecting and promoting the values of the person. The composition of ethics committees must ensure the qualifications and experience necessary to assess the ethical, scientific, and methodological aspects of the proposed studies. The members of the ethics committees must have documented knowledge and experience in clinical trials of medicinal products and medical devices and in other matters within the competence

of the Ethics Committee. In cases of evaluations relating to areas not covered by its own members, the Ethics Committee shall convene, for specific consultations experts from outside the committee for specific advice. The investigator, the sponsor or other personnel participating in the pilot, shall provide, at the request of the committee information on any aspect of the trial. The investigator, the promoter or other trial personnel shall not participate in the decision-making, opinion and voting of the Ethics Committee. For further details, cf. the website in[1].

In Italy, this project is subject to the approval by the Ethical Committee. In order to get the approval, the researchers involved in the project (Dr. Roberta Bevilacqua, Dr. Federico Barbarossa, and Dr. Arianna Margaritini) have to submit a detailed protocol where we declare why the research project is carried out, who are the participants, how we recruit them, which data we ask and manage, what questionnaire are asked, what are the safety and security risks for all the people involved in the study, and other things too. Everything should be explained in detail. The Ethical Committee is specific for Science and Health related studies and interventions and meets monthly. Once the approval is given, the test activities must strictly follow the guidelines declared in the approved protocol. Trial protocol submitted (28.2.2025) at Territorial Ethical Committee is waiting for approval. The ethics committee meeting will take place in the middle of April 2025. Comments on protocol and possible approval by the middle of May 2025.

[1] https://www.gazzettaufficiale.it/eli/id/2013/04/24/13A03474/sg

5 Individual Data management plans

The purpose of the Data Management Plan (DMP) is to provide the TransCare consortium with a guideline to properly manage data (collected, processed and/or generated) throughout the project lifecycle. To ensure proper data management, the consortium will rely on, follow and respect the DMP aiming to ensure the "FAIR" principles (i.e., findable, accessible, interoperable and reusable)[2], and protect the privacy and sensitivity of data (either personal or IoT infrastructure specific research data) against unauthorised access, in compliance with the GDPR[3]. The following principles will be followed.

- (Findable) All generated data will be stored in an easily accessible way by both humans and software, as appropriate. Generally, the generated data falls into two categories: organisational data, which are relevant to the implementation of the innovation actions, and technical and scientific data, including raw and processed experimental data, publications, and software. The generated data within the project will be anonymized, traceable and locatable by means of unique identification mechanisms. All files will be uniquely identifiable by using standardised name conventions and file versioning. When possible, the datasets will be shared in publicly accessible disciplinary repositories, such as Zenodo, using descriptive metadata.
- (Accessible) TransCare will use different tools to make processed data accessible to authorized users and available under well-defined conditions. It involves establishing appropriate access controls, security measures, and data governance policies. Public reports will be shared via public facilities and confidential reports will be shared among the consortia. Data will be accessible between the partners through a common space for the necessary data exchange and communication (e.g., MS Teams). Certain research data considering the demo users are sensitive due to privacy and data protection issues and therefore will be kept confidential or anonymised before being accessible.
- (Interoperable) Suitable standards for data and metadata creation along with appropriate vocabularies will be used to enable seamless integration and interoperability across different systems and platforms. Access will be permitted to authorized users, to use a data copy which may be shared or adapted (remixed, transformed, or build upon existing material). APIs will be used for data exchange facilitation.
- (Reusable) TransCare will adhere to standardized data formats and documentation practices and will promote, when possible, the use open data standards.

The project DMP that uses the THCS template to provide guidance for consortia funded in Transforming Health and Care Systems (THCS) joint transnational calls (JTC) and communicate their strategy concerning research data quality, sharing and security is included as Appendix 1

Next, we present the individual partners from the consortium data management plans, focussing on the main security, privacy, GDPR, etc. principles to be used.

5.1 TUC

TUC will store and process anonymized data in its on-premises server farm in Cluj-Napoca, Romania. TUC has allocated a specific state of the art server for handling TransCare data which is isolated from other research and development activities done in other projects implemented by TUC.

[2] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

[3] https://eur-lex.europa.eu/eli/reg/2016/679/oj

Physical security measures for protecting the data stored and processed on the server:

- The server is in a secured area with fire protection, proper ventilation and cooling
- Only authorized personnel have access to the server room (TUC team researchers)
- Access in the server room is done based on secure key cards, that are kept in a locked office when not used.
- The server room has an allocated alarm system which is permanently activated when authorized personnel are not in the room. Passwords for alarm system are known only by TransCare TUC personnel.
- The server has backup batteries for power outage.

Logical security measures for data protection on TUC server:

- The server HDDs use RAID techniques for backing up data in case of one HDD failure
- The operating system is a Linux kernel is protected through authentication and authorization. Only TransCare TUC personnel has the credentials for accessing the OS level services.
- The communication network uses mechanisms of comprehensive network protection against intrusion such as: IPS (Intrusion Prevention System), firewall and network antivirus filter.
- Remote access to the server is possible only through secured VPN connections and only TUC personnel from the project have credentials and details how to access it.
- The developed ML analytics component will be isolated at the OS level using Docker containers.
- The DB servers (i.e. MySql) deployed on the physical server will be protected against intrusions using password authentication. DB passwords are known only by TUC TransCare personnel.

The data handled in TUC premisses will be received in anonymised format from the Tellu Dialogg app. In the TransCare platform, data will be transferred using REST APIs as JSON messages. To secure data transmission, we will use the HTTPS protocol that uses the TLS protocol to encrypt data. Security of data access or transfer will be achieved using a firewall with appropriate security rules. Also, TUC data handling will consider solutions that eliminate or significantly reduce the system's vulnerability to attacks as recommended in the Open Web Application Security Project (OWASP).

5.2 TLU

Tellu provides the monitoring infrastructure of TransCare, which includes a backend with data storage, web application for management and mobile application for end users. The service for Remote Patient Monitoring from Tellu has been developed according to the principles of data protection by design. The following data management plan is adopted from the service's official privacy policy, as used by Tellu's customers. It is directed at the end user of the system and explains how data privacy is ensured. In the TransCare project, the roles of health organization and health service will be played by each of the trial partners.

5.2.1 The purpose of processing personal data

Remote patient monitoring is a service for people who receive health care from a health organization, such as a municipality, a hospital or a GP, and gives you an easy and safe opportunity to keep health personnel continuously updated on general health, special symptoms and other relevant health information. You as a patient will have an agreement with the health organization about use of the service.

5.2.2 Legal authority for the processing of personal data

The following laws regulate which personal data that can be processed and conditions for processing:

- The Health- and care services Act and the Specialist health services Act give the individual the right to receive healthcare from public health services, and the municipalities and the specialist health service have a duty to provide health care to the individual.
- The health personnel Act requires healthcare personnel to document the healthcare given in medical records.
- The Patient Records Act requires health services to give healthcare personnel access to necessary information of good quality about the patient, as well as ensuring the patient's and users' privacy, patient safety and the right to information and participation.
- The Personal data Act and the General Data Protection Regulation (GDPR) impose the health service (Data controller) and suppliers (Data processors) for sound management of personal data and give the individual patient (the data subject) a number of rights, including the right to access registered personal data, as well as correction and deletion of their data.
- The Patient and user rights Act gives the individual the right to access information that is necessary to gain insight into their health condition and content of the health care provided.

5.2.3 Responsible for data processing

The health service is responsible for providing health services to its inhabitants/patients and is data responsible for all processing of personal data related to the service. The data responsibility entails the responsibility for control measures to ensure that no one has unauthorized access to the personal data.

5.2.4 Processing of personal data

The following describes at a general level how personal data is processed:

- You log in using a secure authentication server. Neither the healthcare service nor Tellu has access to your password or PIN code.
- No personal data is stored on your mobile phone/tablet.
- No personal data is stored on the health personnel's PC/tablet.
- All communication towards the service's central data solution is encrypted.
- All personal data is stored in Norway, encrypted in the health service's health archive at Tellu on behalf of the health service.
- Personal data is stored in the service's central data solution until the health service decides that it should be deleted.

5.2.5 TLU responsibility as supplier and data processor

Tellu is the health service's supplier of software and performs the role of Data Processor in accordance with the data processor agreement between Tellu and the health service. Tellu has developed the service and performs ongoing maintenance and operational services but has no access to personal information unless the health service submits a written request for technical assistance.

5.2.6 TLU subcontractor

Microsoft Azure – owns and operates data center, hardware and backups. Does not have access to personal data.

5.2.7 Report deviation

If you suspect unfortunate or problematic processing of personal data in the service, you must report deviations directly to the health service that is responsible for the health care where this service is

included. The health service will then initiate actions that are necessary to investigate and close deviations.

5.3 KRD

The Memas.app stores information about the user, primarily their contact details, calendar events, the user's reply to questionnaires. We also store a relation to relevant rehabilitation information for the different diagnosis of the user.

The Memas.app client side is hosted by Netlify to ensure scalable and efficient access to the web-client software. The web-client software communicates with our server-backend software.

The server-backend software is hosted by the Google Cloud services in their Helsinki data centre. The server-backend services consist of several dockerized containers with business logic and database-management. The docker-containers are governed by Kubernetes, ensuring scalability and availability to the Memas services. In addition, there is a Loadbalancer and "Cloud armor" providing smart routing to the server-components with available resources, only traffic that meet our "Coud-armor" requirements are allowed to contact the backend services to avoid SSDO attacks and other unwanted traffic that could affect the availability of the Memas-services.

Users of Memas adminweb use Google oAuth authentication for getting access to the services. Users of the Memas app have a personalized 8-digit code for access to their information.

5.4 INRCA

The project committed to the maintenance of participants' anonymity and confidentiality throughout all procedures, including screening, recruitment, testing, evaluation and dissemination procedures. Data collection, usage and storage procedures complied with national laws and the EU's General Data Protection Regulation (GDPR) including the commitment of participants' right to access, right to be informed, right to withdraw, and right to data erasure. Moreover, the servers are in the European Union and compliant to GDPR. Data collection will be compliant with the principle of data minimization i.e. the collection of personal information from study participants will be limited to what is directly relevant and necessary to accomplish the specific goals of the testing and evaluation work packages. Data entry will be carried out using specific software, providing blocks and data entry checks, to reduce the number of entry errors. All screening data will be discarded upon the project completion. During the testing procedures, all visual, auditory and sensory data collected and processed to function as planned will be discarded after the procedures have been completed. The exception to this is the collection of the number of interactions that are logged with each participant. However, these interactions will be anonymous. All research data shall be made openly available for secondary analysis 7 years after the project completion.

5.5 HINS

The study complies with the EU General Data Protection Regulation (GDPR) and national data privacy laws at all stages of its implementation. During enrolment participants will provide written informed consent for study participation, along with explicit agreement for the processing of their personal data. All collected data will be anonymized, with no personal identifiers retained, and securely stored in an encrypted, password-protected Excel spreadsheet accessible exclusively to authorized investigators. To ensure data integrity, automated backups will be performed regularly, while the participants retain the right to withdraw their consent at any time without consequences. In

accordance with institutional data retention policies at HINS all study records will be archived for a period of 10 years following study completion.

5.6 FAR

To comply with GDPR regulations in our study, we follow strict guidelines for handling personal data. We ensure that patients give written consent before their personal data is processed, making sure they are informed and have control over their data. We collect and process only the necessary information to minimize the risk of misuse. To safeguard personal data, we implement robust technical and organizational measures to prevent unauthorized access, loss, or destruction. Patients have the right to access, rectify, delete, and restrict the processing of their personal data, ensuring their privacy and control. When personal data is processed by third parties, we ensure that the data is anonymized, with no personal identifiers retained, and securely stored in an encrypted, password-protected Excel spreadsheet. All study data will be archived for a period of 10 years following study completion according to Norwegian research council recommendations. In addition to complying with GDPR regulations, the municipality adheres to the Norwegian Patient Journal Law for documentation and continuous follow-up of patients. This ensures that patients can receive ongoing care from the municipality even after the completion of the project. The law mandates that patient records are meticulously maintained to facilitate seamless transitions and continuity of care, thereby supporting patients' long-term health and well-being.

6 References

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[2] C. Dantas et. al.: AAL Guidelines for Ethics, Data Privacy and Security. http://www.aal-europe.eu/wp-content/uploads/2020/08/AAL-guidelines-for-ethics-final-V2.pdf
[3] Norwegian National Research Ethics Committees: General guidelines for research ethics. https://www.forskningsetikk.no/en/guidelines/general-guidelines/

Annex 1. TransCare DATA MANAGEMENT PLAN (DMP)

0. Proposal name + project number

TransCare - New care pathways for supporting TRANSitional CARE from hospitals to home using AI and personalised digital assistance.

Project code number in THCS: 1449

1. Description of the data

1.1 Type of study

TransCare main goal is to address transitional care challenges by developing, scaling and validating a digital rehabilitation to a larger number of patients and considering the specific contexts of different healthcare systems in Europe as well as different types of multimorbidity patterns. The project is about alleviating the rehospitalisation period for patient discharged from hospital with an aim to avoid rehospitalisation and reduce the number of human resources and effort in the follow-up care.

Data will be collected and processed from three end-user sites during a 3-month longitudinal study:

- FAR (Farsund municipality) in Norway
- HINS (HEART INSTITUTE "NICULAE STANCIOIU" CLUJ-NAPOCA) in Romania
- INRCA (National Institute of Health and Sciences on Aging) in Italy

1.2 Types of data

In Norway, 80 patients will be recruited. 40 getting TransCare follow-up, the other 40 is a control group followed up according to the present follow-up.

In Romania, 30 patients will be recruited. 15 getting TransCare follow-up, the other 15 is a control group followed up according to the present follow-up.

In Italy, 100 patients will be recruited. 50 getting TransCare follow-up, the other 50 is a control group followed up according to the present follow-up.

The data sample collected during the trial is divided into four macro-categories.

- **Data from clinical and attitudinal scales and measurements**, reported and described within D4.1: Of the participants in the intervention group, information on cognitive and physical status is collected through the administration of Mini Mental State Estimation and Short Physical Performance Battery. In addition, through the CFS scale, the enrolled patient's level of frailty is assessed. In addition, quantitative information is collected on quality of life (EQ-5D-5L) and health impact on everyday life (SF-12), as well as health literacy (eHEALS) and the level of usability of the proposed system (SUS). Finally, semi-structured qualitative interviews will be conducted to understand the level of self-management improvement, usability and effectiveness of the system, and questionnaires on the use of clinical resources to get a comprehensive overview of the patient's impact on the health system as well. The complete list of clinical and non-clinical assessment and scales to be administered is reported in the list below.
- **Data from medical devices**, reported and described within D2.1: The trial system can collect the following data from patients in the trial. Measurement of blood pressure and heart rate with blood pressure meter. Measure of weight with scale. Measurement of oxygen saturation and heart rate with pulse oximeter. Measurement of body temperature with thermometer. Measurement of blood glucose with glucometer. Each end user site organization will select which

measurements to be made by each trial patient, depending on medical condition and available equipment.

- **Data from activity tracker**, also reported and described within D2.1: Trial patients will wear an activity tracker from Fitbit, with data transmitted to Fitbit service. Trial patients can give the project access to some of this data, to be transmitted to and stored in the TransCare system. This includes a heart rate time series and classification of activity level, as well as sleep data (time and duration of sleep phases, breathing rate and oxygen saturation) and daily summary with distance and steps walked, resting heart rate and time spent in different activity levels.
- **Data from well-being form:** For each diagnosis or comorbidity a customized well-being form has been developed. This form is available in the Memas.app. The patient is encouraged to fill in this form on a regular basis.

The data is collected by two components of the TransCare platform, Dialogg from Tellu and Memas from Karde.

Dialogg also collects data from standardised questionnaires that INRCA has collected for the TransCare project. All the assessments, including clinical and non-clinical questionnaires and scales, planned for trial experimentation, are listed below (more details can be found in the corresponding deliverables related to trial protocols):

- Socio-demographic and Anamnesis (Checklist)
- Mini Mental State Estimation (cognitive)
- Short Physical Performance Battery (physical)
- Clinical Frailty Scale (Frailty)
- Assistive Technology Device Predisposition Assessment
- EQ-5D-5L Visual Analogue Scale (quality of life)
- SF-12 short form (impact of health in everyday life)
- Clinical resource utilization questionnaire
- System Usability Scale SUS (Usability of dashboard)
- eHEALS scale
- Semi-structured interview on self-management improvement, usability and effectiveness of the system

Memas collects well-being survey data in the form of a questionnaire with 10 questions per patient. The questions are adapted to the diagnosis of the patient. In Memas, related to the Transcare project, we store the following data:

- Standard contact information about the user
- Results from survey data
- Calendar events

1.3 Format and scale of the data

Data are collected regularly. Activity is monitored continuously by the Fitbit system and transferred to the TransCare system once per day. Medical measurements are collected once or twice per day. Monitored data is transferred by Tellu's Dialogg application (deployed on the patients' smartphone or tablet) into two backend systems of TransCare: TelluCare and ML-based post-discharge analytics.

Dialogg sends measurements to TelluCare in JSON format, as FHIR Observation objects according to the HL7 FHIR standard. This data is stored in a database in the FHIR format. FHIR data is available through an API.

The monitored data is sent as JSON messages through a dedicated API implemented and exposed by the ML-based post-discharge analytics component developed by TUC: (i) intraday Fitbit data, (ii) daily summary data and (iii) other sensors or devices integrated into the remote monitoring platform (e.g. smart blood pressure meter, etc.). This data is stored in TUC server farm located in Cluj-Napoca, Romania in a MySql database. It is further used in the ML pipeline for training, testing and inference processes. The data is interoperable due to the use of the REST API for accessing and due to using standardized JSON messages for transferring it.

Well-being data from Memas is collected once every week per patient through the defined questionnaires. The data are stored in a dGraph database hosted on Google Infrastructure in Helsinki Finland. The data is interoperable due to the use of the REST API for accessing and due to using standardized JSON messages for transferring it.

2. Data collection / generation / reuse

2.1 Will the project reuse data?

Yes ☐ *No* ☒

New data / data management

To run the pilots in a realistic manner and validate the complete TransCare value chain, we will collect data from the recruited patients following GDPR and FAIR principles. For the project trials of three months data collection and management is required to follow good practice and standards. The TransCare project organises its data management plan by project participant or by country. The end user organisations data management plans will focus on the ethical management of user-centric activities. The technical partners' data management plans focus on how monitored data is stored, how data security is achieved, etc. External systems and services that will be used in the research and development work of the project, such as questionnaire applications, will be subject to special procedures, including privacy information to informants, anonymised responses as well as denial of access to other informants' responses. Individual data management plans are reported in the corresponding project deliverable concerning ethics and data management.

2.2 Methodologies for data collection / generation

Data collected through co-creation and evaluation phases with end-users will all be collected anonymously and shared with technical partners. The aim of the data sharing is to develop an improved technology solution which will grasp the end-users' conditions and needs. Existing data that will be reused in the project include responses to questionnaires, transcripts of text, responses to qualitative questions, video and pictures taken during interviews (only if the publication consent is signed by the represented users).

For Memas, the data is collected from users using the Memas app. For each diagnosis, incl. comorbidities, a well-being questionnaire with 10 questions is defined. When a carer sets up the Memas app for the patient, he/she selects the diagnosis the patient is undergoing rehabilitation for. The corresponding questionnaire becomes available in the Memas app, ready to be filled out by the patient.

For Dialogg the data are collected either from sensors and medical devices or from recruited patients through questionnaires. Data is provided through standard questionnaire templates or automatically from devices using standard protocols like BLE. Data is stored based on the standard HL 7 FHIR data

model.

Related to the ML analytics component developed by TUC, data generated as output of the algorithms is exposed to Tellu platform through secured APIs using JSON standard. It uses the same security and privacy principles as the other data models used by the ML component.

2.3 Data quality and standards

Consistency and quality of the collected data are based on applying certified medical devices. The data collection and transfer to the cloud-based system is controlled by the Personal Health Gateway software stack. All data (such as measurements and replies to questionnaires) are verified by health personnel. Any strange or suspicious data will be deleted, and it will be requested to repeat the procedure for collecting data (e.g., by providing a new measurement)

3. Data management, documentation and curation

3.1 Managing, storing and curating data.

In TransCare different types of databases are used for storing data. The different database servers are either cloud based or on premisses (e.g. MySql). In both situations the database servers assure state of the art DB security principles by default.

Memas well-being data are stored securely at the Google Datacenter in Helsinki Finland.

In TelluCare data are stored in Azure data centre in Norway, and it is continuously backed up in another geolocation in Norway. Data will be deleted after the project end. Data will be stored according to the HL7 FHIRE data model.

TUC will store and process data in its premises in Cluj-Napoca, Romania. TUC has allocated a specific state of the art servers for handling TransCare data which is isolated from other research and development activities done in other projects implemented by TUC. The data will be used in anonymized manner as input for ML algorithms. The server HDDs use RAID techniques for backing up data in case of one HDD failure. Also, a backup service moves data weekly on a secured replication server. Data curation (pre-processing) for the ML algorithms is done through semi-automatized and secured processes starting from the anonymized received monitored data.

Responsibilities for the data management

Data collected by Memas are managed by Karde. Data are backed up regularly. Karde is not curating data in its systems.

Data is processed and managed by Tellu that has the role of Data Processor. The data owners are the respective pilot owner (FAR, HINS and INRCA).

3.2 Metadata standards and data documentation

Data stored in TelluCare will be stored according to the HL FHIR semantic data model. The metadata are according to the standard.

3.3 Data preservation strategy and standards

The collected data will be deleted at the project end. If the Data Owner request to sustain any of the collected data, this data will be maintained in a new regime completely independent from the TransCare project and under full responsibility of the Data Owner.

3.4 Allocation of resources

Using FAIR (Findable, Accessible, Interoperable, Reusable) principles for data management involves different cost components, which can vary depending on the scope of data preservation. In TransCare we will not preserve data after the TransCare-project is finished, thus no costs for long-term data

preservation are required. While the costs generated during project lifecycle for FAIR data are difficult to estimate, we address them as follows:

- Data Management and Infrastructure Costs: data storage, curation and maintenance will be done by the consortium partners personnel involved in the project; the infrastructures for data storage will be the ones already available and operating at each partner, being shared for TransCare usage.
- Human Resource Costs: are covered through the personnel costs allocated to each partner in the general budget table
- Licensing of tools: the consortium uses open-source tools; the proprietary licenses that are used are the ones already available and supported by the organizations in the consortium

4. Data security and confidentiality of potentially disclosive information

4.1 Formal information/data security standards

In the TransCare, anonymized data is shared using REST APIs using the JSON standard. To secure data transmission, technical partners will use the HTTPS protocol that uses the TLS protocol to encrypt data. Data handling considers solutions that eliminate or significantly reduce the system's vulnerability to attacks as recommended in the Open Web Application Security Project (OWASP). For the cloud environment (e.g. Microsoft's Azure or Google cloud platforms), the high security requirements of ISO 27001 are used and assured by the cloud provider. For on premises data storage (e.g. TUC servers) specific security principles are employed.

Tellu is certified according to ISO 27001, registration number 274925-2018-AIS-NOR-UKAS.

4.2 Main risks to data security

During the trials personal data will not be requested. The data handled in TransCare will be received are stored in anonymised format from the end-user sites in Italy (INRCA), Romania (HINS) and Norway (FAR). No sensitive data is stored in the TransCare platform. Among the security techniques available, data pseudonymisation or anonymisation is highly recommended by the GDPR regulation. Such techniques reduce risk to the confidentiality and security of information related to human participants and assist "data processors" in fulfilling their data compliance regulations. Additionally, to mitigate the risk different security measures will be used such as authentication and authorization for digital access, encryption for data transmission, physical security for digital/physical data access (e.g. password/key based access for rooms, locked drawers, etc.). Only authorized personnel have access to the data in the TransCare project.

5. Data sharing and access

During the trials monitored data will be securely stored, access being provided through Tellu web platform for healthcare professionals and through Dialogg app for the patients. Additionally, questionnaire data from Memas application will be accessed by patient directly through the application. Programmatically data is made available through HTTPS based APIs to other software components such as the ML analytics for further processing.

The clinical, psycho-social, and attitudinal data described in Section 1.2 of the present document and collected through the administration of measurement scales during each evaluation times, will be organized organically and will be shared with partners for analysis during and after the trial in an anonymized form following what is required by the international regulation on data processing and privacy.

Specifically, Italian researchers will collect all information within MS Excel documents stored on their hardware and protected by password encrypting. When these are transmitted to other partners, keys

will be used to open the documents.

All sensitive information will be removed so that anonymity is guaranteed and the participant who generated the clinical and nonclinical data set cannot be traced.

5.1 Suitability for sharing

If relevant, datasets with monitored data or ML analytics results will be shared in publicly accessible disciplinary repositories, such as Zenodo, using descriptive metadata. Trials results data can be also shared as an analysis of the scales, metrics or indicators results. Anonymized data will be used.

5.2 Discovery by potential users of the research data

The partners in the project will aim for publishing open-access scientific papers describing the intent of the project, the data collected and the processing of data.

Similar information will in a condensed form be published on the project's Facebook, LinkedIn and website.

Well known repositories (e.g. Keggle, Zenodo) can be used for publishing research data. They can be easily accessed by researchers.

5.3 Governance of access

The TransCare-consortium will use open access principles for sharing data. Decision for sharing non-open access data to potential users will be taken according to the government bodies from the CA.

Well known repositories (e.g. Keggle, Zenodo) can be used for sharing TransCare resulting research data.

5.4 The study team's exclusive use of the data

As mentioned above, relevant research data publishing will be made under open access principles. We will follow open science practices in line with the Horizon Europe principles. TransCare will offer open access to its scientific publications by ensuring open access, selecting either self-archiving/'green' open access or open access publishing/'gold' open access, to facilitate dissemination and reuse of the project's results.

5.5 Restrictions or delays to sharing, with planned actions to limit such restrictions

Our approach to confidentiality is to protect the TransCare by building appropriate access rights, encryption, anonymisation, and provenance techniques into the core models of the platform. During piloting, all personnel involved including system evaluators, service providers, etc., sign a confidentiality agreement to maintain the privacy of involved persons and their information. Where necessary, their information will be anonymised. Relevant research data will be anonymized in preparation for wider dissemination at the end of the study/project. If, for any reason, it is not possible to anonymize part of the data, it will not be disseminated.

5.6 Regulation of responsibilities of users

Generally we will follow open access principles as mentioned above but if required to use agreements we can use the standard ones such as CC BY-NC-ND 4.0: Creative Commons Attribution-Non-commercial-No Derivatives that allows users to copy and distribute the material in any medium or format in un-adapted form only, for non-commercial purposes only, and only so long as attribution is given to the creator.

6. Responsibilities

Considering the general management procedures for consortium bodies apart for each partner PI the following managers will be responsible for data management, creation, security and quality: (i) the Impact Manager (Terje Grimstad) that leads the general dissemination and exploitation actions, in order

to maximize the exploitation potentials for project results and (ii) Local Ethics Managers (Italy - Federico Barbarossa, Norway - Camilla Gabrielsen, Romania - Ovidiu Anchidin) that deal with regulations for data security arrangements and that of handling person (-al)/sensitive data, and privacy.

7. Relevant institutional, departmental or study policies on data sharing and data security	
Policy	**URL or Reference**
Data Management Policy & Procedures	European Commission, "EC H2020 Programme, Guidelines on FAIR Data Management in Horizon 2020, Version 3.0," 2016. [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf. European Parliament and the Council, "General Data Protection Regulation (GDPR) - EU 2016/679," 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj
Data Security Policy	C. Dantas et. al.: AAL Guidelines for Ethics, Data Privacy and Security. http://www.aal-europe.eu/wp-content/uploads/2020/08/AAL-guidelines-for-ethics-final-V2.pdf
Data Sharing Policy	Open science in Horizon Europe, https://rea.ec.europa.eu/open-science_en
Institutional Information Policy	N/A
Other	Norwegian National Research Ethics Committees: General guidelines for research ethics. https://www.forskningsetikk.no/en/guidelines/general-guidelines/

8. Author of this Data Management Plan (Name) and, if different to that of the Principal Investigator, their **phone number & email contact details**
Dr. Riitta Hellman, Karde. Tel: +47 98 21 12 00 E-Mail: rh@karde.no