Co-funded by the Horizon 2020
Framework Programme of the European Union

Deliverable 1.5
Final version Legal/Ethical Monitoring and Review

Work Package 1: Data protection, Ethical Impact and Interoperability

affecTive basEd iNtegrateD carE for betteR Quality of Life: TeNDER Project

Grant Agreement ID: 875325

Start date: 1 November 2019

End date: 30 April 2023

Funded under programme(s): H2020-SC1-DTH-2018-2020/H2020-SC1-DTH-2019

Topic: SC1-DTH-11-2019 Large Scale pilots of personalised & outcome based integrated care

Funding Scheme: IA - Innovation action

Disclaimer

The TeNDER consortium consists of the following Partners.

Table 1 - Consortium Partners List

No	Name	Short name	Country
1	UNIVERSIDAD POLITECNICA DE MADRID	UPM	Spain
2	MAGGIOLI SPA	MAG	Italy
3	DATAWIZARD SRL	DW	Italy
4	UBIWHERE LDA	UBI	Portugal
5	ELGOLINE DOO	ELGO	Slovenia
6	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	Greece
7	VRIJE UNIVERSITEIT BRUSSEL	VUB	Belgium
8	FEDERATION EUROPEENNE DES HOPITAUX ET DES SOINS DE SANTE	HOPE	Belgium
9	SERVICIO MADRILENO DE SALUD	SERMAS	Spain
10	SCHON KLINIK BAD AIBLING SE & CO KG	SKBA	Germany
11	UNIVERSITA DEGLI STUDI DI ROMA TOR VERGATA	UNITOV	Italy
12	SLOVENSKO ZDRUZENJE ZA POMOC PRI DEMENCI - SPOMINCICA ALZHEIMER SLOVENIJA	SPO	Slovenia
13	ASOCIACION PARKINSON MADRID	APM	Spain

Document Information

Project short name and Grant Agreement ID	TeNDER (875325)
Work package	WP1: Data protection, Ethical Impact and Interoperability
Deliverable number	D1.5
Deliverable title	Final version Legal/Ethical Monitoring and Review
Responsible beneficiary	VUB
Involved beneficiaries	All
Type[1]	Report
Dissemination level[2]	Public
Contractual date of delivery	30/04/2023
Last update	27/04/2023

[1] **R:** Document, report; **DEM:** Demonstrator, pilot, prototype; **DEC:** Websites, patent fillings, videos, etc.; **OTHER**; ETHICS: Ethics requirement; ORDP: Open Research Data Pilot.

[2] **PU:** Public; **CO:** Confidential, only for members of the consortium (including the Commission Services).

Document History

Version	Date	Status	Authors, Reviewers	Description
V0.1	14/09/2021	Draft	Danaja Fabcic Povse, Paul Quinn (VUB)	Questionnaires on the second impact assessment
V0.2	3/12/2021	Draft	All partners	Partner answers to the second impact assessment questionnaires
V0.3	14/01/2022	Draft	Danaja Fabcic Povse (VUB)	Data analysis and definition of mitigation measures
V0.4	26/09/2022	Draft	Danaja Fabcic Povse (VUB)	Initial questionnaires for the third impact assessment
V0.5	26/10/2022	Draft	Danaja Fabcic Povse (VUB)	Revised questionnaires for the third impact assessment and request for partner input
V0.6	2/12/2022	Draft	SPO, UNITOV, APM, SERMAS, SKBA, MAG, CERTH, UBI, ELGO	Partner answers to the 3rd impact assessment questionnaires
V0.7	15/12/2022	Draft	UPM, DW	Partner answers to the 3rd impact assessment questionnaires
V0.8	23/01/2023	Draft	Danaja Fabcic Povse (VUB)	Data and risk analysis
V0.9	27/02/2023	Draft	Danaja Fabcic Povse, Paul Quinn (VUB)	Internal check
V0.10	30/03/2023	Draft	Nicholas Vretos, Vassilis Solaichidis (CERTH)	Technical description of pilots in sections 2.1 and 3.1
V0.11	30/3/2023	Draft	Danaja Fabcic Povse (VUB)	Consistency and editorial check
V0.12	10/04/2023	Draft	Jorge Alonso (UPM)	Peer review

V0.13	26/04/2023	Draft	Agostino Chiaravalotti (UNITOV)	Peer review
V0.14	27/04/2023	Draft	Danaja Fabcic Povse, Paul Quinn (VUB)	Final draft

Acronyms and Abbreviations

Acronym/Abbreviation	Description
AD	Alzheimer's disease
CVD	Cardiovascular disease
DoA	Description of action
EEA	European Economic Area (EU27+Norway, Liechtenstein, Iceland)
EU	European Union
ICT	Information and communication technologies
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
MDR	Medical Devices Regulation
RBG	Red, green, blue
TeNDER	TeNDER, affecTive basEd iNtegrateD carE for betteR Quality of Life; funded by grant agreement No 875325
WP	Work package
WP29	Article 29 Working Party, an advisory body to the European Commission (replaced by the European Data Protection Board-EDPB)

Contents

List of Tables

Executive Summary

In the TeNDER project, legal and ethical work focuses on data protection and privacy, treatment of human participants in pilots, wider societal concerns, and regulation of medical devices, including their essential health and safety requirements. Following up on the findings of the first impact assessment, contained in the D1.4 First version Legal/Ethical Monitoring and Review, we provide a risk-aware roadmap on addressing legal and ethical risks stemming from the second and third waves of pilots with TeNDER patients. As such, **this deliverable goes beyond the legal requirements of art. 35 of the General Data Protection Regulation (GDPR)**, which requires controllers to carry out a data protection impact assessment when the processing is likely to result in a high risk to the rights and freedoms of natural persons.

The second impact assessment addresses concerns such as eventual **third party data processing**, the **retaining of data inside the EEA**, and processing of data that are not **relevant, adequate or necessary** for a given purpose. The third impact assessment responds to the risks concerned the **profiling of patients** and **automated decision-making**, the respective roles of **human and automated** (machine) **decision-making** both with regards to data processing and medical decisions, and the risk of non-compliance with the **medical devices regime** should TeNDER in the future be used as a medical device.

This report also provides recommendations to future adopters regarding continuous legal and ethical monitoring, as well as recommendations for mitigation measures for protecting patients' data protection and privacy interests.

The recommendations include:

1. Involving stakeholders in the development and monitoring processes
2. Clear terminology with little to no difficult legal language
3. Carrying out an impact assessment beyond art. 36 of the GDPR to provide a wider lens through which developers can ethically assess medical technologies
4. Technical and organisational measures to foster privacy and data protection
5. Context-appropriate use of cameras and/or other intrusive technologies
6. Enable patients to turn the devices off when they wish to do so
7. Mitigation measures for using third-party devices
8. Continuous impact assessments

The results of continuous monitoring processes will serve to inform **similar future projects** in the field of **e-health, remote patient care and health tech**. We advise the reader to also consult the TeNDER D1.6 Final version of fundamental rights, which contains broader implications of TeNDER for law, policy and future adopters.

1 Introduction

1.1 Purpose and scope

The current deliverable is part of T1.3, Continuous Legal/ethical Monitoring and Review. The aim of the deliverable is to monitor the impacts of TeNDER on the requirements identified in WP1 and WP2, as the ICT solutions are integrated, tested and evaluated. This will ensure that any new aspect or update of the TeNDER solutions or their potential application is tested against the relevant societal concerns, described in T7.1. The monitoring will be performed by VUB, who will have the right to access any information arising from the work of the project, to attend any meeting of the consortium and to interfere should it consider the work of the consortium incompatible with TeNDER. Monitoring compliance is an ongoing task in the TeNDER project, which began with the D1.1, First Version of Fundamental Rights, Ethical and Legal Implications and Assessment, continued in the D1.4, which assessed and evaluated the efforts leading up to the first wave of the TeNDER pilots in the context of the identified framework.

Based on the questionnaires of the three impact assessments, the current deliverable provides a risk-aware roadmap to ensuring legal and ethical requirements have been met in the second and third waves. The impact assessment reports on consequences of actions taken in the project, in order to identify potential benefits and adverse effects, and allow the consortium to take the most beneficial actions.

1.2 Contribution to other deliverables

The findings of our work in T1.3 is tightly connected to the work in T1.1, especially the D1.6 Final version of fundamental rights, ethical and legal implications and assessment. Both tasks address the development process of TeNDER and its legal and ethical implications in order to provide a comprehensive picture of regulatory challenges such projects present in practice.

1.3 Structure of the document

The first two sections present the impact assessments of the second and third wave of pilots, including the motivation, methodology, risk assessment and response (i.e., mitigation measures). Each impact assessment consists of four sections related to data protection, privacy and socio-ethic risks as well as risks relating to the use of medical devices. Finally, the results of the impact assessments and the conclusions and recommendations thereof are summarised.

2 Second TeNDER impact assessment

2.1 Motivation

In the TeNDER project, the technical development and medical research activities are carried out in close connection with legal and ethical work. In order to address possible concerns arising from the consortium's work, impact assessment reports are provided as means of addressing the consequences for participants' fundamental rights and broader socio-ethical aspects.

The first impact assessment, whose results have been published in the D1.4, reported on the technical development and the set-up of the first round of pilots. Here, we present the second impact assessment which follows the set up and execution of the second wave of pilots, reflecting the project development before M25 (November 2021). The exercise will be carried out again before the end of the project in order to reflect future development and evaluate our approach. In this manner, the experience of TeNDER impact assessment can inform policy-makers, industrial best practices and academic researchers.

Main technical changes between the first and the second waves

In the first wave, almost all the sensors had been integrated into the TeNDER system and components that analyze and summarize the acquired data had been developed. In addition, initial version of the web and mobile interfaces had been designed and integrated in the system.

In the second wave, the technical updates involved a) the support of additional sensors (binary and environmental), b) the upgrade and improvement of the performance of existing components in terms of speed and accuracy taking also account the users' comments from the first wave (e.g. addition of new exercises in the rehabilitation tool, improvement of accuracy of fall detection), c) the creation of new components (e.g. , virtual assistant) based on the DoA requirements and plan, d) update of web and mobile interfaces based on the users' needs.

2.2 Methodology

The second impact assessment is part of T1.3 in WP1 Data Protection, Ethical Impact and Interoperability of the TeNDER project. In the context of WP1, the aim of the impact assessment is to identify the risks related to social, ethical, legal and privacy issues and suggest the measures to mitigate them. The analysis of these risks consists of the following stages:[3]

- Defining and describing the legal and ethical framework applicable to TeNDER's developments and activities (resulted in D1.1 – First Fundamental rights, ethical and legal implications and assessment);
- Conducting the first impact assessment in TeNDER to identify and respond to initial legal and ethical risks likely to occur in the first wave of pilots;
- Conducting the second impact assessment, taking into account the new project developments and the different functionalities used in the second wave, as opposed to the first wave, such as the system recommender. As in the first impact assessment, our work has three stages:

[3] For a comprehensive discussion of methodology in impact assessments, including legal literature and validated applied projects methodologies, see TeNDER, 'D1.4, "First Version Legal/Ethical Monitoring and Review"' (2021) <https://www.tender-health.eu/>.

- Preparing questionnaires addressed to the partners to collect the information on their activities in the project and their impact from legal, privacy and ethical perspectives;
- Collecting and clarifying the answers of partners;
- Identification, analysis and description of social, legal, ethical and privacy risks, and measures to mitigate them.

The probability of risk to occur has been rated using a three-grade scale:

- **Remote** – Risk nature is known but no known occurrences of the risk happened in similar activities. Depending on the nature of the risk, the risk can be ignored, although a preventive action may still be proposed.
- **Possible** – Risks of similar nature have happened in similar activities or the situation may be conducive to the occurrence of the risk. A response plan should be suggested in case the risk manifests.
- **Probable** – There is a significantly high chance that risk will occur, or the situation is favourable to occurrence of risks. Mitigating actions should be discussed and monitored.

The identified risks may have an impact with respect to social, legal, ethical and privacy issues. The scale used to rate the impact is the following:

- **Minimal** – In case of occurrence, the risk does not hinder on any relevant interests, e.g., safety, or the rights and freedoms of the individual, thus no modification or adaption is needed. It is also possible that the occurrence of the risk only requires minor adaptations.
- **Significant** – In case of occurrence, interests, rights and freedoms of the individual are affected, thus hindering the goals of the project. Significant revision and re-orientation may be necessary.
- **Severe** - In case of occurrence, interests, rights and freedoms of the individual are severely affected, meaning that the project will not achieve one or more goals. The activity or the functionality may be unlawful or contrary to ethical principles. This warrants for substantial revision and re-orientation of the project.

As mentioned above, the risks are classified according to different areas. The number of relevant risks identified per category is as follows:

- Data protection: 15 risks
- Privacy: 6 risks
- Ethical and societal: 5 risks
- Risks related to the use of medical devices: 4 risks

Finally, measures are suggested to mitigate the identified risks. These measures take into account legal and ethical requirements, the activities carried out by partners and the facilities they have, and the probability and impact of the risk. Importantly, the risks are assessed and the measures to mitigate them are suggested in relation to the project's objectives. At this phase, the project activities are focused on developing prototype solutions rather than commercialising them. This aspect is taken into consideration in the risk response plan and enables the use of more controllable solutions. However, the impact assessment is a continuous process and if the context of project's activities is changed, the necessary updates in the risk response plan will be made. Moreover, consideration is also given at the exploitation of the TeNDER system upon completion of its development. While the risks might arise in different areas and are related to different project activities, the mitigating measures have been assigned to specific partners; in most cases, it is VUB as the leader of WP1 and the partner responsible for the WP or task where the risk might occur.

2.3 Risk assessment and response

2.3.1 Data protection risks

The table below presents the identified data protection risks and measures to mitigate them:

- Identifies the risks that might occur in the second wave when personal data are processed by the TeNDER consortium (**name and description**).
- How likely they are to occur (**probability of occurrence**) and what would be their **impact** on patients' rights.
- How the consortium commits to avoid the risk from occurring (**risk response plan**), or to answer the risk if it occurs, and which partners will be **responsible** for the risk mitigation action.

Table 2 - Risks related to the Protection of Personal Data (2nd wave)

RISKS RELATED TO THE PROTECTION OF PERSONAL DATA						
Risk ID	**Name**	**Description**	**Probability of occurrence**	**Impact**	**Risk response plan**	**Responsible partner**
LAWFULNESS, FAIRNESS AND TRANSPARENCY						
DP.1	Consent lacks informativeness	TeNDER involves a wide range of technologies developed and operated by different partners. The technologies are connected to each other and operated both separately and commonly as part of the TeNDER ecosystem. Additionally, the project involves different data subjects and different pilots. The variety of all these elements as	Possible	Significant	Prior to starting the pilots, the patients involved in the research signed consent forms (D10.3), which were accompanied by information sheets in the patients' own languages, as well as simplified informed consent forms. If necessary, the consent and/or information forms can be changed, adapted or amended to reflect the project developments in order to ensure transparency	VUB, user partners

		well as the complexity of technologies might create difficulties for a data subject to understand the flows of their personal data and subjects involved in the processing. This affects both lawfulness and transparency of data processing.			toward patients and other users.	
PURPOSE LIMITATION						
DP.2	Purpose of data processing is not clearly defined	The purpose of personal data processing is conducting the research activities in the project. However, due to the complexity of the second wave, the mentioned purpose is deemed to be too wide and might lack sufficient specification	Possible	Severe	The general purpose will be layered to sub-purposes and accompanied with clear description of the project and its goals (in informational sheets, on the website). This will ensure that the purpose is detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied.	Partner processing the data + VUB
DP.3	Processing of personal data outside the	The project's pilots will engage	Possible	Severe	While engaging patients and providers in pilots	Partner(s) processing

	scope of the purpose it was collected for	healthcare providers already actively engaged with their patients. In this case, some of their personal data is already being processed by the respective partners. Depending on the description of initial purposes of data processing, it might be incompatible with processing activities in the project			or other project activities, the conditions of their data processing (including purpose, legal basis, processing activities) will be defined separately from the existing processing activities in their organisation. This will enable compatibility with the purpose.	the data + VUB
DATA MINIMIZATION						
DP.4	Processing of data not necessary for the purposes	TeNDER collects data through diverse technologies, with the purpose of developing new functionalities. It is possible that some functionalities could be developed and tested without the need to process personal data	Possible	Severe	Analyse the necessity of using data in the existing technologies (sensors, microphone etc.) vis-a-vis functionalities developed in the second wave (fall detection, emotion detection tools etc.), including whether functionalities could be developed using non-personal data	VUB + partners involved in data processing
DP.5	Collected personal data are not relevant or not adequate for the purposes	Personal data collected in the second wave are low quality (e.g., camera or microphone	Possible	Significant	A data management plan has been drafted (WP2), which inter alia addresses the	VUB + partners involved in data processing

		footage), or cannot be machine-read, and cannot be used to train algorithms and/or develop the functionalities			quality, interoperability and data formats, ensuring the data can be used as planned. Data that are not adequate ot relevant to achieve the purposes will be deleted by the involved partners.	
INTEGRITY AND CONFIDENTIALITY						
DP.6	Insufficient security of data processing, transfer and storage	TeNDER's technical architecture is complex and will include different layers and several means of collecting and processing data (several types of devices, local COPs, hardware, middleware). This all might create the security risks such as risks of data loss, breach of confidentiality)	Possible	Severe	In every scenario where the High-level services of TeNDER do not require the identification of a certain person, data can be anonymised (if relevant, also aggregated) for analysis and evaluation. All data from/to TeNDER platform are transited over encrypted sessions (ex. HTTPS). Details on anonymisation processes are given in D10.7	Technical partners
DP.7	Storage of data in the cloud	The TeNDER technical architecture will include internet cloud layer. Cloud technologies in general might pose some risks related to security of data stored there	Possible	Severe	Defining what kind of data can be stored in the cloud is necessary. In addition, the security, pseudonymisation and anonymization techniques will be used. Data access is protected by	VUB + MAG

					Keycloak authentication and authorisation mechanisms and only logged-in users with specific permissions can access it. Further details on data storage in the cloud will be decided by the TeNDER partners in the next stages of the project.	
STORAGE LIMITATION						
DP.8	Different periods of data storage	TeNDER includes different partners processing different types of personal data and with regards to different processing activities. Partners might store the personal data for different periods of time	Probable	Significant	The TeNDER partners shall agree on the minimum and maximum periods for storing personal data to ensure respect of the storage limitation principle, taking into account applicable national legislation.	VUB + all partners
ACCOUNTABILITY						
DP.9	The roles of partners are not clearly defined	Involvement of almost all partners in processing of personal data with respect to different purposes and activities creates the risk of lack of accountability (‘everyone is responsible for everything’=’no	Minimal/ possible	Severe	All partners shall define their role (controller/ processor of personal data), the partners they cooperate with and how. They will specify the purposes of data processing, types of data and relevant activities, as laid out in the Deliverable D1.1 and the Data	VUB + all partners

		one is responsible')			Sharing Agreements	
DP.10	Access to data by unauthorized subjects	TeNDER includes different companies, organisations and universities. While some representatives are continuously involved in the project activities and are informed on the necessary procedures, other employees might get access to the data not being aware of the rules of its protection	Possible	Severe	TeNDER partners have taken high-level measures to ensure access controls and other organisational and technical measures to ensure data is not access by unauthorised parties. High-level measures are described in D10.6 and was further determined in the D2.4 (delivered M19). As required by art. 30 of the GDPR, partners shall keep the record of processing activities describing the type of data processed, by whom (including the person within organization) and for which purpose. The scope and amount of people having access to the personal data shall be limited.	VUB + partners whose servers have been breached
RESPECT OF DATA SUBJECTS' RIGHTS						
DP.11	Limited right to erasure of personal data	If conditions of art. 17(1) GDPR are met, the patient or other data subject can request	Possible	Significant	Evaluate whether the personal data collected are still necessary to achieve the goal, whether consent has been revoked	VUB + user and technical partners involved in the specific

		deletion of their data			and if other criteria in art. 17 of the GDPR are met	data processing
DP.12	Limited data portability	It is not defined if the data processed within TeNDER might be technically transferred to another data controller under the request of data subject	Probable	Low	This issue is likely to occur post-project rather than during the project research phase. Right to portability will be evaluated in the light of upcoming EU policies (the scope and nature of the right and its relevance for TeNDER users); this evaluation will if relevant be included in the final legal assessment and recommendations report (D1.6).	Entity exploiting TeNDER
OTHER RISKS						
DP.13	Processing of participants' personal data by parties external to the consortium	TeNDER partners are using certain services and products offered by external providers for specific purposes (e.g. wearables from Fitbit, Nuitcrack for skeleton detection, EUSurvey etc.), and the external parties could gain access to participants' data	Possible	Severe	A number of mitigation measures has been taken by partners: dedicated email addresses, dedicated devices, using fake dates of birth (e.g., January 1 of the year in which the patient was born), no real names are disclosed, synchronising is turned off and accounts are not connected to social media service providers.	Partners involved in the processing + VUB
DP.14	Transfer of personal data	Some external service	Possible	Severe	Due diligence in choosing the	All partners + VUB

	outside the EEA by external service providers	providers (e.g. providers of devices) chosen may be based outside the area covered by the GDPR i.e., European Economic Area (EEA), or may transfer participants' personal data outside this area			devices and service providers based on their privacy policies and data practices. Only providers whose data centres are based in the EEA have been chosen, with the exception of FitBit (used by UPM). In this case, no identifiable data (name, date of birth) will be shared with the service provider, and dedicated email addresses have been set up for this purpose.	
DP.15	Risks related to processing of personal data of caregivers	TeNDER will implement technologies aimed to monitor the health status of patients and this ensures their safety. However, it is likely that caregivers might need to disclose their own personal data, such as name, email address, workplace, etc. to use the device.	Probable	Significant	The system is based on different roles (patient, professional caretaker, informal caretaker etc.). The division of roles prevents or allows access to specific types of personal data. Legal grounds for such data processing: processing is necessary in order to protect the vital interests of the data subject or of another natural person; or necessary for the purposes of the	VUB + all partners

					legitimate interests pursued by the controller or by a third party.	

2.3.2 Privacy risks

As described in the First Fundamental rights, ethical and legal implications and assessment (D1.1), the right to privacy is a fundamental right guaranteed by international treaties (such as the Universal Declaration of Human Rights), at the level of the Council of Europe (the European Convention of Human Rights) and the European Union (the Charter of Fundamental Rights of the European Union). The right to privacy means that *everyone has the right to respect for his or her private and family life, home and communications. This right might be limited only in cases provided by law and with respect the essence of the right (subject to the principle of proportionality).* Privacy is a complex concept and might include different aspects. In addition to those described in the First Fundamental rights, ethical and legal implications and assessment (D1.1), several types of privacy are identified:[4]

- **privacy of the person** *(*encompasses the right to keep body functions and body characteristics private);
- **privacy of behaviour and action (**concerns activities that happen in public space, as well as private space and might include sensitive issues such as sexual preferences and habits, political activities and religious practices);
- **privacy of communication** (aims to avoid the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording and access to e-mail message);
- **privacy of thoughts and feelings** (people have a right not to share their thoughts or feelings or to have those thoughts or feeling revealed. Individuals should have the right to think whatever they like);
- **privacy of location and space** (the right to move about in public or semi-public space without being identified, tracked or monitored. This conception of privacy also includes a right to solitude and a right to privacy in spaces such as the home, the car or the office);
- **privacy of association** (concerned with people's right to associate with whomever they wish, without being monitored).

The table below presents the identified privacy risks and measures to mitigate them.

- Identifies the risks that might occur in the project scenario when personal data are processed by the TeNDER consortium (**name and description**).
- How likely they are to occur (**probability of occurrence**) and what would be their **impact** on patients' rights.

[4] Rachel L Finn, David Wright and Michael Friedewald, 'Seven Types of Privacy' in Serge Gutwirth and others (eds), *European Data Protection: Coming of Age* (Springer Netherlands 2013) <https://doi.org/10.1007/978-94-007-5170-5_1> accessed 22 June 2020. Also see FASTER, p. 17.

- How the consortium commits to avoid the risk from occurring (**risk response plan**), or to answer the risk if it occurs, and which partners will be **responsible** for the risk mitigation action.

Table 3 - Privacy Risks (2nd wave)

PRIVACY RISKS						
Risk ID	**Name**	**Description**	**Probability of occurrence**	**Impact**	**Risk response plan**	**Responsible partner**
P.1	Affecting privacy through the use of cameras	During some pilots, cameras (RGB/Azure) will be used in skeleton view to evaluate movement and support the patient in case they fall, or a similar emergency occurs	Probable	Significant	The camera records the skeleton only, not the individual as a whole. The recordings will not be identifiable without additional data, which is kept separately.	User partners using cameras (UNITOV, SERMAS, SKBA, SPO, APM)
P.2	Affecting privacy through the use of microphone	Microphone will be one of the sensors used to help monitor patients. Apart from the voice of the patient, a microphone could pick up the voices of other users (care-givers, family members, casual visitors etc.)	Probable	Significant	There will be no covert monitoring, and third parties will be aware of the ongoing use of microphone. Special arrangements can be made e.g. when receiving visitors and family members.	User partners using microphones (UNITOV, SERMAS, SKBA, SPO) in cooperation with VUB and technical partners
P.3	Affecting privacy of person through	Comprehensive monitoring of patients through the use of different	Probable	Significant	Patient monitoring will be limited in	VUB + all partners

	individualized bio-monitoring of patients	sensors (Audio/microphone, Fitbit, Kinect camera, RGB sensor, Localisation sensor, sleep tracker, binary sensor)			scope. Biosensor devices such as portable devices will be used to measure heart rate, body temperature, blood glucose or blood pressure, but not other aspects of the private life which fall outside the scope of the TeNDER project. Moreover, health records will not be included in the Slovenian pilot. Finally, the invasiveness of technology in the piloting is being constantly evaluated by all partners involved.	
P.4	Affecting privacy of the participants through emotion	Emotion detection tool will be developed and tested during the second wave. The	Probable	Significant	Use of appropriate microphone, careful selection of	All partners

	detection tool	performance might interfere with participants' privacy by monitoring through the microphone to determine the patient's mood through the tone of their voice			relevant datasets, limited data storage periods by the technical providers	
P.5	Affecting privacy of the participants through recommender tool	Recommender tool will be developed and tested during the second wave. The performance might interfere with participants' privacy. This tool serves to suggest relevant actions to the care-giver.	Probable	Significant	Privacy interferences such as monitoring and data collection will be limited to what is strictly necessary to achieve the objective.	All partners
P.6	Affecting privacy of the participants through fall detection tool	Fall detection tool will be developed and tested during the second wave. The performance might interfere with participants' privacy	Probable	Significant	Use of only the appropriate sensors and skeleton cameras, which contain no identifiable information. Only the caregiver will be alerted to the patient's fall.	All partners

2.3.3 Ethical and societal risks

The general framework for ethical and societal concerns arising out of TeNDER are initially described in the First Fundamental rights, ethical and legal implications and assessment (D1.1). As set out in D1.1, there are a number of different factors related to the TeNDER project that can give cause to ethical and/or societal concerns. One of these concerns relates to the participation of vulnerable groups in scientific research. Furthermore, the use of new technologies, their acceptance by the

society and trust in such technologies is something to assess and consider. Finally, the balancing of various fundamental rights and vital interests of different groups of people is another.

In TeNDER, informational awareness shall include the technologies used in the project, the corresponding risks, benefits and the way to use them. This will enable all groups to make informed decisions, which increases the safety and trust in the technologies used. The ethical and societal risks that might arise out of the project and the measures to mitigate them are described in the table below:

- Identifies the risks that might occur in the project scenario when personal data are processed by the TeNDER consortium (**name and description**).
- How likely they are to occur (**probability of occurrence**) and what would be their **impact** on patients' rights.
- How the consortium commits to avoid the risk from occurring (**risk response plan**), or to answer the risk if it occurs, and which partners will be **responsible** for the risk mitigation action.

Table 4 - *Ethical and Societal Risks (2nd wave)*

ETHICAL AND SOCIETAL RISKS						
Risk ID	**Name**	**Description**	**Probability of occurrence**	**Impact**	**Risk response plan**	**Responsible partner**
E.1	Lack of trust in the use of new technologies from the side of users	Lack of trust in new technologies if users do not understand how those technologies work, or why they are necessary/useful.	Remote	Severe	Training, explanation, user-friendly interfaces for both the patient and the care-giver	VUB + all partners, especially partners involved in front end/UX development
E.2	Lack of trust in the technologies by society	Lack of trust in new technologies is a common issue as people do not fully understand how the technologies work and what might be the side effects.	Remote	Significant	TeNDER will be designed according to safety requirements and in full respect of applicable legislation and bioethical principles Transparency toward the user on risks and benefits	Entity exploiting TeNDER
E.3	Affecting the fundamental	When equipment is installed in the	Probable	Minimal	Some parts of the system	VUB + all partners

	rights of people not participating in the pilot/using the TeNDER system	pilot sites, there is an inherent risk that the sensor, camera, depth sensors or microphone will pick up activity from others than those participating in the pilot/using the technology - one person's desire to use such assistive technology in a group setting may infringe upon another's right to privacy or the other person may object to the use of a certain device or equipment			cam distinguish between the users and others in accessing data. The other person is aware of the monitoring technology being used (the device is not concealed). Moreover, partners will aim not to implement sensors in shared or public spaces.	
E.4	Use of assistive technology for people with neurodegenerative illnesses such as PD and AD	In the case of dementia and other neurodegenerative illnesses, the people using the technology are not necessarily able to fully understand the implications and may not have the capacity to give full consent or where its use may result in shame, stigma and embarrassment, yet its use may be beneficial, enabling them to accomplish tasks that they would otherwise be unable to manage	Possible	Significant	Co-design process with users (WP2), usability assessment in WP6 and D7.1. Inter alia, the co-design process will adapt the technology's material features, affordances, and aesthetic properties; a distributed knowledge of the individual and the places they visited; and a collective and dynamic	VUB + all partners

					interpretation of risk. Post-pilot surveys will be conducted to evaluate users' (especially patients') experience. Providing transparency and information to the users, which are adapted to the level of understanding appropriate to the specific patient (consent forms given in D10.3)	
E.5	Participants suffer harm from mis-diagnosis performed by TeNDER technologies	Data collected by TeNDER technologies could be used as grounds for diagnoses of various illnesses. However, the data could lead to a wrong diagnosis, which could have serious consequences for participants' health and lives.	Low	Severe	During TeNDER pilots, the users and stakeholders are closely involved with technological development and their usefulness in diagnostic procedures. Moreover, the patients who enrol in pilots have already been treated at relevant clinics/hospitals, and are less likely to be	All partners

					misdiagnosed. However, this is a risk that is more likely to occur in a post-project setting.	

2.3.4 Risks related to the use of medical devices

The table below presents the identified risks related to the use of medical devices and measures to mitigate them.

- Identifies the risks that might occur in the project scenario when personal data are processed by the TeNDER consortium (**name and description**).
- How likely they are to occur (**probability of occurrence**) and what would be their **impact** on patients' rights.
- How the consortium commits to avoid the risk from occurring (**risk response plan**), or to answer the risk if it occurs, and which partners will be **responsible** for the risk mitigation action.

Table 5 - Risks related to the Use of Medical Devices (2nd wave)

RISKS RELATED TO THE USE OF MEDICAL DEVICES						
Risk ID	**Name**	**Description**	**Probability of occurrence**	**Impact**	**Risk response plan**	**Responsible partner**
MD.1	Non-compliance with Medical Devices Regulation (MDR)[5]	A medical device is any device (or instrument, software, implant or any article) intended to be used for medical purposes. If a device falls under this definition, it must meet the occupational	Possible	Severe	The partners will monitor the applicability of the Medical Devices Regulation, keeping in mind the main purpose of the TeNDER technology being developed. The main goal of the technology developed is to assist the people in their decision-making; it serves	VUB + all partners

[5] Regulation 2017/745 of 5 April 2017 on medical devices.

		health & safety requirements as mandated by the regulation, before it can be put on the European Union market.			to warn and monitor, and not treat illnesses or disabilities, which does not seem to fall under the MDR's scope of application. As part of the co-design process and pilot evaluation, the partners will consider the notions of 'manufacturer', the definition of a 'medical device', and the purpose they want to attribute to the OSHW project.[6] The applicability of the MDR to the end product will also be revisited in the D1.6.	
MD.2	Use of unsafe medical devices	The device or technology used in the project poses a safety risk to the user (patient or care giver).	Minimal	Significant	All sensors used in TeNDER have a CE mark. Devices have been used extensively and the user experience has been largely positive.	Technical partners
MD.3	Information conveyed by the device does not assist in health monitoring, warning or evaluation	A malfunction of the device due to low battery, poor connection or similar technical problem, resulting in	Possible	Significant	The partners involved will carry out a technical examination of the malfunction and correct it (e.g. replace battery, adapt settings, connect	Technical and user partners (depending on the source of malfunction)

[6] Elisabetta Biasin and Erik Kamenjašević, 'Open Source Hardware and Healthcare Collaborative Platforms: Common Legal Challenges' (2020) 4 Journal of Open Hardware 7.

		broken data flow (no reminders, notifications, alerts…)			device to the network…) Check whether the device is being used properly (e.g. whether the patient takes it outside with them)	
MD.4	Safety risks for the participants	Participants could be injured while using the technologies and devices	Possible	Low	The devices present little danger to their users, a possible scenario being that the participant drops the device and hurts themselves in the process. Should accidents become common, partners will re-evaluate the use of devices.	User partners

3 Third TeNDER impact assessment

3.1 Motivation

The third impact assessment provide a risk-aware roadmap to tackling legal and socio-ethical challenges that could possibly stem from the third wave of TeNDER pilots. It also presents the final impact assessment of TeNDER as a research project and inspires recommendations for future research.

Main technical changes between the second and the third waves

In the third wave, the technical updates involved a) the upgrade and improvement of the performance of existing components in terms of speed and accuracy taking also account the users' comments from the previous wave (e.g. improvement of accuracy of virtual assistant), b) the creation of new components (alerts, audio-, video-, multimodal based emotion recognition, virtual assistant) based on the DoA requirements and plan , c) creation of new components based on the users' needs (e.g. task scheduler for the rehabilitation scenario, monitoring server collecting status information regarding data acquisition), d) web and mobile interfaces in order to visualize the new information that TeNDER system creates and updates based on the users' needs (e.g. graphs and statistics).

3.2 Methodology

To avoid unnecessary repetition, the reader of the third impact assessment can consult the methodology sections above, since the consortium has consistently adopted the same methodology in all three impact assessments.

The number of relevant risks identified per category is as follows:

- Data protection: 18 risks
- Privacy: 3 risks
- Ethical and societal: 3 risks
- Risks related to the use of medical devices: 2 risks

3.3 Risk assessment and response

3.3.1 Data protection risks

The table below presents the identified data protection risks and measures to mitigate them:

- Identifies the risks that might occur in the second wave when personal data are processed by the TeNDER consortium (**name and description**).
- How likely they are to occur (**probability of occurrence**) and what would be their **impact** on patients' rights.
- How the consortium commits to avoid the risk from occurring (**risk response plan**), or to answer the risk if it occurs, and which partners will be **responsible** for the risk mitigation action.

Table 6 - Risks related to the Protection of Personal Data (3rd wave)

RISKS RELATED TO THE PROTECTION OF PERSONAL DATA						
Risk ID	**Name**	**Description**	**Probability of occurrence**	**Impact**	**Risk response plan**	**Responsible partner**
LAWFULNESS, FAIRNESS AND TRANSPARENCY						
DP.1	Consent lacks informativeness	TeNDER involves a wide range of technologies developed and operated by different partners. The technologies are connected to each other and operated both separately and commonly as part of the TeNDER ecosystem. Additionally, the project involves different data subjects and different pilots. The variety of all these elements as well as the complexity of technologies might create difficulties for a data subject to understand the flows of their personal data and subjects involved in the processing. This affects both lawfulness and transparency	Possible	Significant	The same mitigation measures as in the prior two waves apply, namely the prior informed consent procedures for patients (D10.3), accompanied by information sheets in the patients' own languages, as well as simplified informed consent forms.	VUB, user partners

		of data processing.				
PURPOSE LIMITATION						
DP.2	Purpose of data processing is not clearly defined	The purpose of personal data processing is conducting the research activities in the project. However, due to the complexity of the third wave, the mentioned purpose is deemed to be too wide and might lack sufficient specification	Possible	Severe	Same mitigation measures apply as in the prior waves, such as layered purpose, clear description of the project and its goals, contained inter alia in information sheets pursuant to art. 13 and 14 GDPR, and on the website.	Partner processing the data + VUB
DP.3	Processing of personal data outside the scope of the purpose it was collected for	The project's pilots will engage healthcare providers already actively engaged with their patients. In this case, some of their personal data is already being processed by the respective partners. Depending on the description of initial purposes of data processing, it might be incompatible with processing activities in the project	Possible	Severe	Same mitigation measures apply as in the prior waves. Namely, the project-contextual processing is defined separately from the existing processing activities in their organisation. This will enable compatibility with the purpose.	Partner(s) processing the data + VUB
DATA MINIMIZATION						

DP.4	Processing of data not necessary for the purposes	TeNDER collects data through diverse technologies, with the purpose of developing new functionalities. It is possible that some functionalities could be developed and tested without the need to process personal data	Possible	Severe	Same mitigation measures apply as in the prior waves, including analyses whether the use of non-personal data could contribute to the same goals.	VUB + partners involved in data processing
DP.5	Collected personal data are not relevant or not adequate for the purposes	Personal data collected in the third wave are low quality, or cannot be machine-read, or cannot be used to develop the functionalities such as recommender, user interface etc.	Possible	Significant	Same mitigation measures apply as in the prior waves, including a data management plan (WP2), and deletion of data that are not adequate or relevant to achieve the purposes.	VUB + partners involved in data processing
INTEGRITY AND CONFIDENTIALITY						
DP.6	Insufficient security of data processing, transfer and storage	TeNDER's technical architecture is complex and will include different layers and several means of collecting and processing data (several types of devices, local COPs, hardware, middleware). This all might create the security risks	Possible	Severe	Same mitigation measures apply as in the prior waves In every scenario where the High-level services of TeNDER do not require the identification of a certain person, data can be anonymised (if relevant, also aggregated) for analysis and evaluation. All	Technical partners

		such as risks of data loss, breach of confidentiality)			data from/to TeNDER platform are transited over encrypted sessions (ex. HTTPS). Details on anonymisation processes are given in D10.7	
DP.7	Storage of data in the cloud	The TeNDER technical architecture will include internet cloud layer. Cloud technologies in general might pose some risks related to security of data stored there	Possible	Severe	Same mitigation measures apply as in the prior waves Defining what kind of data can be stored in the cloud is necessary. In addition, the security, pseudonymisation and anonymization techniques will be used. Data access is protected by Keycloak authentication and authorisation mechanisms and only logged-in users with specific permissions can access it.	VUB + MAG
STORAGE LIMITATION						
DP.8	Different periods of data storage	TeNDER includes different partners processing different types of personal data and with regards to different processing activities. Partners might store the personal data	Probable	Significant	Same mitigation measures apply as in the prior waves regarding the minimum and maximum periods for storing personal data to ensure respect of the storage limitation principle, taking into account applicable	VUB + all partners

		for different periods of time			national legislation.	
ACCURACY						
DP.9	Inaccurate patient data	Since the third wave involves many patients, their medical records and data collected through the dedicated technologies must be accurate for each respective patients.	Possible	Significant	TeNDER researchers ensure that devices such as bands and sensors are not used for multiple patients. Should inaccuracies arise, measures can be taken to rectify the inaccurate data.	User partners
ACCOUNTABILITY						
DP.10	The roles of partners are not clearly defined	Involvement of almost all partners in processing of personal data with respect to different purposes and activities creates the risk of lack of accountability (‘everyone is responsible for everything’=’no one is responsible’)	Minimal/ possible	Severe	Same mitigation measures apply as in the prior waves All partners have defined their role (controller/ processor of personal data), the partners they cooperate with and how, as laid out in the Deliverable D1.1 and the Data Sharing Agreements	VUB + all partners
DP.11	Access to data by unauthorized subjects	TeNDER includes different companies, organisations and universities. While some representatives are continuously involved in the project activities and are informed on the	Possible	Severe	Same mitigation measures apply as in the prior waves TeNDER partners have taken high-level measures to ensure access controls and other organisational and technical measures to ensure data is not access by unauthorised	VUB + partners whose servers have been breached

		necessary procedures, other employees might get access to the data not being aware of the rules of its protection			parties. High-level measures are described in D10.6 and was further determined in the D2.4 (delivered M19). As required by art. 30 of the GDPR, partners shall keep the record of processing activities describing the type of data processed, by whom (including the person within organization) and for which purpose. The scope and amount of people having access to the personal data shall be limited.	
RESPECT OF DATA SUBJECTS' RIGHTS						
DP.12	Limited right to erasure of personal data	If conditions of art. 17(1) GDPR are met, the patient or other data subject can request deletion of their data	Possible	Significant	Same mitigation measures apply as in the prior waves Evaluate whether the personal data collected are still necessary to achieve the goal, whether consent has been revoked and if other criteria in art. 17 of the GDPR are met	VUB + user and technical partners involved in the specific data processing
DP.13	Limited data portability	It is not defined if the data processed within TeNDER might be	Probable	Low	This issue is likely to occur post-project rather than during the	Entity exploiting TeNDER

		technically transferred to another data controller under the request of data subject			project research phase.	
OTHER RISKS						
DP.14	Processing of participants' personal data by parties external to the consortium	TeNDER partners are using certain services and products offered by external providers for specific purposes (e.g. wearables from Fitbit, Nuitcrack for skeleton detection, EUSurvey etc.), and the external parties could gain access to participants' data	Possible	Severe	Third party services are used minimally in the third wave. Where necessary, the same measures as in the second wave apply e.g. dedicated email addresses, dedicated devices, using fake dates of birth, no real names are disclosed, synchronising is turned off and accounts are not connected to social media service providers.	Partners involved in the processing + VUB
DP.15	Transfer of personal data outside the EEA by external service providers	Some external service providers (e.g. providers of devices) chosen may be based outside the area covered by the GDPR i.e., European Economic Area (EEA), or may transfer participants' personal data outside this area	Possible	Severe	Due diligence in choosing the devices and service providers based on their privacy policies and data practices. Identical mitigation measures as in the second wave.	All partners + VUB

DP.16	Profiling and automated decision-making	Profiling refers to automated processing of personal data to evaluate personal aspects relating to a patient (art. 4(4) of the GDPR). Patients have the right to not be subject to automated decision-making in specific instances (art. 22 of the GDPR).	Possible	Severe	In TeNDER only general profiling in the sense of the WP29 opinion[7] is used – the purpose is to build patient profiles based on which recommendations are given to improve their quality of sleep or daily movement. There is no automated decision-making in the sense of the above cited opinion. More information can be found in the D1.6	VUB + all partners
DP.17	Automated decision-making leading to legal or significant effects for the patient	Solely automated decision-making based on profiling Sensitive PD – not allowed unless explicit consent or substantial public interest	Minimal	Severe	TeNDER system is explicitly built with a human as decision-maker in mind. The functionalities tested in the third wave do not in any way make legal or other significant decisions affecting the patients, but rather provide a data overview or summary of a patient's condition, which is then used by the patient or the caregiver to	VUB + all partners

[7] Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2018) WP251rev.01 <https://ec.europa.eu/newsroom/article29/items/612053>.

					decide accordingly.	
DP.18	Risks related to processing of personal data of caregivers	TeNDER will implement technologies aimed to monitor the health status of patients and this ensures their safety. However, it is likely that caregivers might need to disclose their own personal data, such as name, email address, workplace, etc. to use the device.	Probable	Significant	Same mitigation measures apply as in the prior waves.	VUB + all partners

3.3.2 Privacy risks

The table below presents the identified privacy risks and measures to mitigate them.

- Identifies the risks that might occur in the project scenario when personal data are processed by the TeNDER consortium (**name and description**).
- How likely they are to occur (**probability of occurrence**) and what would be their **impact** on patients' rights.
- How the consortium commits to avoid the risk from occurring (**risk response plan**), or to answer the risk if it occurs, and which partners will be **responsible** for the risk mitigation action.

Table 7 - Privacy Risks (3rd wave)

PRIVACY RISKS						
Risk ID	**Name**	**Description**	**Probability of occurrence**	**Impact**	**Risk response plan**	**Responsible partner**
P.1	Unrestricted use of monitoring	Technologies such as the ones used in TeNDER can be	Probable	Significant	Limit the use of technology	User + technical partners

	technology affecting patient privacy	used for patient monitoring in ways that a patient finds particularly invasive (e.g., inside their home or bedroom), or continuously without the option to temporarily or permanently stop the monitoring,			to specific time and place (e.g. only used in rehabilitation room for the exercises) The patient can turn off the device if they desire without loss of future functionalities.	
P.2	Privacy impacted due to sharing of information with third parties	Technologies used share patient information with third parties of which patients are not aware or do not agree with.	Minimal/ possible	Significant	Aside from third-party service providers (see above DP.14 and DP.15) patient data is not shared with external entities. Where third party services are used, mitigation measures continue to allow patients to keep control over their privacy.	All partners
P.3	Impact on privacy of third parties while they are in the same area as	Care staff, visitors and family members may feel that their privacy is being affected when they visit the	Minimal	Significant	Devices such as sensors and FitBits only collect information	User + technical partners

	the patient involved in TeNDER	patient using TeNDER technologies.			from their assigned patient and nobody else.	

3.3.3 Ethical and societal risks

The ethical and societal risks that might arise out of the project and the measures to mitigate them are described in the table below:

- Identifies the risks that might occur in the project scenario when personal data are processed by the TeNDER consortium (**name and description**).
- How likely they are to occur (**probability of occurrence**) and what would be their **impact** on patients' rights.
- How the consortium commits to avoid the risk from occurring (**risk response plan**), or to answer the risk if it occurs, and which partners will be **responsible** for the risk mitigation action.

Table 8 - Ethical and Societal Risks (3rd wave)

ETHICAL AND SOCIETAL RISKS						
Risk ID	**Name**	**Description**	**Probability of occurrence**	**Impact**	**Risk response plan**	**Responsible partner**
E.1	Technology developed does not bring societal benefits	Technology does not improve the quality of patients' life (e.g., connectivity and easier overview of wellbeing, symptoms etc.)	Minimal	Severe	In the most general sense, technology is a practice that solves a problem. Should the societal problem – care-taking for patients with AD, PD or CVD no longer be a problem for example because a cure has been found, then TeNDER would not bring a	All partners + future TeNDER adopters

					societal advantage. Until such a cure is discovered and widely available, however, TeNDER technology can bring benefits.	
E.2	Lack of trust in the use of new technologies from the side of users	Lack of trust in new technologies if users do not understand how those technologies work, or why they are necessary/useful.	Remote	Severe	Training, explanation, user-friendly interfaces for both the patient and the care-giver	VUB + all partners, especially partners involved in front end/UX development
E.3	Usability and safety risks to users (patients, caregivers)	Physical or other harm to the participants and their caregivers associated with the use of technology	Minimal	Significant	Patients may not know how to use a smartphone, which can be remedied by an explanation from the TeNDER researcher or caregiver. User manuals can be distributed or trainings given to answer specific questions from patients. There are no specific safety risks, though a phone may	Partner(s) using the device

					fall and break.	

3.3.4 Risks related to the use of medical devices

The table below presents the identified risks related to the use of medical devices and measures to mitigate them.

- Identifies the risks that might occur in the project scenario when personal data are processed by the TeNDER consortium (**name and description**).
- How likely they are to occur (**probability of occurrence**) and what would be their **impact** on patients' rights.
- How the consortium commits to avoid the risk from occurring (**risk response plan**), or to answer the risk if it occurs, and which partners will be **responsible** for the risk mitigation action.

Table 9 - Risks related to the Use of Medical Devices (3rd wave)

RISKS RELATED TO THE USE OF MEDICAL DEVICES						
Risk ID	**Name**	**Description**	**Probability of occurrence**	**Impact**	**Risk response plan**	**Responsible partner**
MD.1	Non-compliance with Medical Devices Regulation (MDR)[8]	A medical device is any device (or instrument, software, implant or any article) intended to be used for medical purposes. If a device falls under this definition, it must meet the occupational health & safety requirements as mandated by the	Possible	Severe	The partners will monitor the applicability of the Medical Devices Regulation, keeping in mind the main purpose of the TeNDER technology being developed. The main goal of the technology developed is to assist the people in their decision-making; it serves to warn and monitor, and not treat illnesses or disabilities, which does not seem to	VUB + all partners

[8] Regulation 2017/745 of 5 April 2017 on medical devices.

		regulation, before it can be put on the European Union market.			fall under the MDR's scope of application. As part of the co-design process and pilot evaluation, the partners consider the notions of 'manufacturer', the definition of a 'medical device', and the purpose they want to attribute to the OSHW project.[9] The applicability of the MDR to the end product will also be revisited in the D1.6.	
MD.2	Information conveyed by the device does not assist in health monitoring, warning or evaluation	A malfunction of the device due to low battery, poor connection or similar technical problem, resulting in broken data flow (no reminders, notifications, alerts…)	Possible	Significant	The partners involved will carry out a technical examination of the malfunction and correct it (e.g. replace battery, adapt settings, connect device to the network…) Check whether the device is being used properly (e.g. whether the patient takes it outside with them)	Technical and user partners (depending on the source of malfunction)

[9] Biasin and Kamenjašević (n 7).

4 Findings, conclusions and recommendations

In the impact assessments for the second and third waves of pilots, we analysed the risks to fundamental rights of patients and addressed wider societal concerns, relevant to TeNDER research and development. We went beyond the requirements of art. 35 of GDPR in order to present a comprehensive picture of how fundamental rights are likely to be affected by our work, and how to respond appropriately.

The main legal and ethical risks associated with TeNDER research and development relate to data protection, privacy, socio-ethical aspects and the use of medical devices. *In the first wave*, the main risks (identified in our previous report – D1.4 First version of legal/ethical monitoring and review) related to providing relevant information to patients, preventing processing of data that are unnecessary, inadequate or irrelevant for the given purpose, as well as the need to continuously address legal requirements in the future.

In this report, we addressed some of those concerns as well as specific ones regarding the second and the third waves. Specifically, *in the second wave* the main concerns stemmed from eventual third party data processing, the retaining of data inside the EEA, and processing of data that are not relevant, adequate or necessary for a given purpose. *In the third wave*, the risks concerned the profiling of patients and automated decision-making, the respective roles of human and automated (machine) decision-making both with regards to data processing and medical decisions, and the risk of non-compliance with the medical devices regime should TeNDER in the future be used as a medical device. As in the previous two waves, maintaining the appropriate relationship between the patient data and the purpose of their processing has been very important. Patients' data should not be used outside the purpose they were collected for, or they are not relevant, adequate or necessary for the given purposes.

General recommendations for future adopters regarding continuous legal and ethical monitoring:

1. Development and monitoring should be carried out side-by-side and involve all stakeholders in the process. In the case of TeNDER, this included users who presented the patients' perspectives and preferences, technical partners and a legal and ethical expert.
2. Terminology should be as clear as possible. The questionnaires provided herein have been reviewed by all types of partners involved and present an opportunity for a cross-discipline conversation with little to no "legalese", i.e. difficult legal language. The clearer the questions in an impact assessment, the more informative the answers will be.
3. The three impact assessments of TeNDER go beyond the requirements laid out in art. 36 of the GDPR and can thus serve to provide a wider lens through which to view medical technologies than a minimally compliant data protection impact assessment as required by the Regulation.

Recommendations for mitigation measures for protecting patients' data protection and privacy interests: [10]

1. Apply technical as well as organisational measures to the developed technologies, such as using different tools in appropriate contexts (e.g., cameras in the rehabilitation room rather

[10] Fabcic Povse D, 2023, 'Challenges of remote patient care technologies under the General Data Protection Regulation: preliminary results of the TeNDER project', Harvard University/Cambridge University Publishing (in print).

than in patients' homes), as well as legal solutions (e.g., applying additional safeguards to ensure informedness of the consent)

2. Keep data in the EHR accurate and up to date; respond to patient requests for rectification of their medical information.
3. If using cameras or other especially intrusive technologies, consult the patients on their placement within the room and inform on the possibility to turn the device off.
4. When using third-party devices and opting out of data sharing is desired but not possible (e.g., in the case of wearables), use mitigation measures, such as using pseudonyms instead of names, approximate date of birth, not connecting the device to social media presence etc.
5. Continuous legal and ethical monitoring via impact assessments and other (ad hoc) communication

The results of continuous monitoring processes will serve to inform similar future projects in the field of e-health law, remote patient care and health tech. We advise the reader to also consult the TeNDER D1.6 Final version of fundamental rights, which contains broader implications of TeNDER for law, policy and future adopters.

References

Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2018) WP251rev.01 <https://ec.europa.eu/newsroom/article29/items/612053>

Biasin E and Kamenjašević E, 'Open Source Hardware and Healthcare Collaborative Platforms: Common Legal Challenges' (2020) 4 Journal of Open Hardware 7

Fabcic Povse D, 2023, 'Challenges of remote patient care technologies under the General Data Protection Regulation: preliminary results of the TeNDER project', Harvard University/Cambridge University Publishing (in print)

Finn RL, Wright D and Friedewald M, 'Seven Types of Privacy' in Serge Gutwirth and others (eds), *European Data Protection: Coming of Age* (Springer Netherlands 2013) <https://doi.org/10.1007/978-94-007-5170-5_1> accessed 22 June 2020

TeNDER, 'D1.4, "First Version Legal/Ethical Monitoring and Review"' (2021)

TeNDER, 'D1.5, "Final version of fundamental rights, ethical and legal implications and assessment"' (2023)

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)

Regulation 2017/745 of 5 April 2017 on medical devices

Annex I: Second Impact Assessment – Questionnaire for Coordinating Tech Partners

1.1 Questions related to your role in the second wave

1. Will your organisation develop any technology (or component) for the second wave or contribute thereto?
   If yes, please name and describe it.

2. Will your organisation use any existing technology for the second wave?
   If yes, please name and describe it and the purpose of its use. Also specify the source of the technology (own, another TeNDER partner or external tech provider-which one).

3. Will your organisation process or intend to process personal data on behalf of the data controlling partners in the TeNDER consortium in the context of the second wave? If so, what types of data?
   Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, erasure or destruction. This includes the processing of pseudonymised data. For more details on the terms 'personal data' and 'processing', please see D1.1 (section 4.3.3.1). For examples of categories of data please see question 4.

1.2 Data protection

4. What types of data will be collected and processed by the TeNDER system?
Where possible, please separate this with respect to the relevant technologies and other data collecting methods (e.g. xx data is collected with xx sensor, xx component will process xx data). The categories below are provided as an example.

a. Identification data (e.g. name, last name, data of birth, age, gender, email, phone)
b. Personal features
c. Financial data
d. Physical, physiological or behavioural characteristics of a natural person, allowing or confirming their unique identification (please specify)
e. Genetic data
f. Biometric data
g. Other information regarding health, incl. mental health
h. Habits
i. Family composition
j. Hobbies and interests
k. Consumption patterns
l. Residence or home address
m. Education
n. Occupation and employment
o. Social security number
p. Racial or ethnic background
q. Philosophical or spiritual orientation
r. Information on sexual preferences
s. Political orientation or opinion
t. Membership of trade union or affiliation
u. Other memberships
v. Video footage
w. Other, namely:

If possible, fill in the planned collection/processing of data by technology, and specify method of collection/processing:

a) Sensors
b) Wearables
c) Kinect microphone
d) Kinect camera
e) Other technology

5. Whose personal data is being processed?
Please describe the data subjects, i.e. the (groups of) individuals whose personal data will be collected and processed.

6. What is the legal basis for processing of personal data?

7. What is the purpose of processing the data and what are the expected benefits?

a) Sensors b) Wearables c) Kinect microphone d) Kinect camera e) Other technology

8. How long will the personal data be retained? What will happen with the personal data after the second wave? Please define per technology, where possible.

a) Sensors b) Wearables c) Kinect microphone d) Kinect camera e) Other technology

9. What kind of security measures will you take to ensure security of personal data? Please define per technology, where possible.

a) Sensors b) Wearables c) Kinect microphone d) Kinect camera e) Other technology

10. How will data gathered in the functionalities being tested contribute to development of:

- Fall detection tool

Source of data	Sensors	Wearables	Kinect microphone	Kinect camera	Other technology

How will data from this source contribute to development of the fall detection tool?					

- Emotion detection tool

Source of data	Sensors	Wearables	Kinect microphone	Kinect camera	Other technology
How will data from this source contribute to development of the emotion detection tool?					

- Recommender

Source of data	Sensors	Wearables	Kinect microphone	Kinect camera	Other technology
How will data from this source contribute to development of the recommender?					

11. Is the processing of personal data really necessary to achieve the purpose identified above? Would other means (mock data, anonymous data set, fewer variables of personal data) be less satisfactory to achieve the same outcome? Please specify per technology:

a) Fall detection tool
b) Emotion detection tool
c) Recommender

12. Does the technology being used transfer any data to actors external to the consortium (e.g. the service provider, cloud host)? If yes, are they based inside or outside the EEA, and where?

a) Sensors

b) Wearables
c) Kinect microphone
d) Kinect camera
e) Other technology

13. If the above answer is yes, what kind of mitigation measures can you adopt to protect the personal data of TeNDER patients?

a) Use a comparable technology that does not involve transfer of data to other jurisdictions
b) Opt-out of data sharing with service provider
c) Use the device offline/without internet connection
d) Do not use real names
e) Do not use real birthdates
f) Do not connect to social media profile(s)
g) Use a dedicated email address
h) Use a dedicated device
i) Other measure(s), namely:

1.3 Privacy

14. In order to minimise the impact on privacy, can the use of the technology be limited to a specific time or place, e.g. it can be turned off by the patient?

15. When the service is provided by an external entity (not part of the consortium), is opting out of data sharing possible? If yes, how? Can it easily be done by the patient?

16. If opt-out is not possible, can you use other measures e.g. dedicated emails, dedicated devices, etc.?

a) Opt-out of data sharing with service provider
b) Use the device offline/without internet connection
c) Do not use real names
d) Do not use real birthdates
e) Do not connect to social media profile(s)
f) Use a dedicated email address

g) Use a dedicated device
h) Other measure(s), namely:

17. How can the privacy of third parties, e.g. visitors or other staff be protected, while they are in the same area as the patient involved in TeNDER?

1.3 Socio-ethical aspects

18. What do you think will be the claimed benefit for the user of the technology and general society, regarding the second wave of pilots?

19. Are there any safety risks for the users related to the use of the technology in the second wave?

20. What kind of skills, training and information will be needed for the end-users of this technology?

21. What technical measures might be implemented to assist end-users in a better and faster understanding the technology? What measures can be taken to ensure the right and efficient use of the technology?

22. What other measures could be taken to increase trust of society and individuals in the use of the technology?

1.4 Development of medical technology

23. Will technology be developed that monitors the health status of end-users? If yes, in what way?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

24. Will technology be used that monitors the health status of end-users? If yes, in what way?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

25. Does the technology help prevent, diagnose or provide a prognosis of an illness, injury or disability? If yes, how?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

26. Does the technology send data to health care providers to monitor an illness, injury or disability? If yes, how?

d) Fall detection tool
e) Emotion detection tool
f) Recommender

27. Does the technology suggest some type of treatment or provide some type of alleviation for an illness, injury or disability? If yes, how?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

28. Will the technology used in the second wave be used for any of the following purposes: diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of AD, PD or CVD? If yes, how?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

29. Upon receiving the recommendation from technology, will the decision to diagnose, prevent, monitor, etc. be taken by a human caretaker, or by the technology itself? What is the role of the caretaker in the decision-making process?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

30. Will you use any technology marked with CE and if so, which technology(-ies)?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

31. Do you plan to adopt the CE marking for the technology used in the second wave, and if so, for which technology(-ies)?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

Annex II: Second Impact Assessment – Questionnaire for Tech Partners

1.1 Questions related to your role in the second wave

1. Will your organisation develop any technology (or component) for the second wave or contribute thereto?

If yes, please name and describe it.

2. Will your organisation use any existing technology for the second wave?
If yes, please name and describe it and the purpose of its use. Also specify the source of the technology.

3. Will your organisation process or intend to process personal data on behalf of the data controlling partners in the TeNDER consortium in the context of the second wave? If so, what types of data?
Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, erasure or destruction. This includes the processing of pseudonymised data. For more details on the terms 'personal data' and 'processing', please see D1.1 (section 4.3.3.1). For examples of categories of data please see question 4.

1.2 Data protection

4. What types of data will be collected and processed by the TeNDER system?
Where possible, please separate this with respect to the relevant technologies and other data collecting methods (e.g. xx data is collected with xx sensor, xx component will process xx data). The categories below are provided as an example.

x. Identification data (e.g. name, last name, data of birth, age, gender, email, phone)
y. Personal features
z. Financial data
gg. Hobbies and interests
hh. Consumption patterns
ii. Residence or home address
jj. Education
kk. Occupation and employment

aa. Physical, physiological or behavioural characteristics of a natural person, allowing or confirming their unique identification (please specify)
bb. Genetic data
cc. Biometric data
dd. Other information regarding health, incl. mental health
ee. Habits
ff. Family composition
ll. Social security number
mm. Racial or ethnic background
nn. Philosophical or spiritual orientation
oo. Information on sexual preferences
pp. Political orientation or opinion
qq. Membership of trade union or affiliation
rr. Other memberships
ss. Video footage
tt. Other, namely:

If possible, fill in the planned collection/processing of data by technology, and specify method of collection/processing:

a) Sensors b) Wearables c) Kinect microphone d) Kinect camera e) Other technology

5. Whose personal data is being processed?
Please describe the data subjects, i.e. the (groups of) individuals whose personal data will be collected and processed.

6. What is the legal basis for processing of personal data?

7. What is the purpose of processing the data and what are the expected benefits?

f) Sensors g) Wearables h) Kinect microphone i) Kinect camera j) Other technology

8. How long will the personal data be retained? What will happen with the personal data afterwards?

a) Sensors
b) Wearables
c) Kinect microphone
d) Kinect camera
e) Other technology

9. What kind of security measures will you take to ensure security of personal data?

a) Sensors
b) Wearables
c) Kinect microphone
d) Kinect camera
e) Other technology

10. How will data gathered in the functionalities being tested contribute to development of:

- Fall detection tool

Source of data	Sensors	Wearables	Kinect microphone	Kinect camera	Other technology
How will data from this source contribute to development of the fall detection tool?					

- Emotion detection tool

Source of data	Sensors	Wearables	Kinect microphone	Kinect camera	Other technology
How will data from this source contribute to					

development of the emotion detection tool?					

- Recommender

Source of data	Sensors	Wearables	Kinect microphone	Kinect camera	Other technology
How will data from this source contribute to development of the recommender?					

11. Is the processing of personal data really necessary to achieve the purpose identified above? Would other means (mock data, anonymous data set, fewer variables of personal data) be less satisfactory to achieve the same outcome? Please specify per technology:

d) Fall detection tool
e) Emotion detection tool
f) Recommender

12. Does the technology being used transfer any data to actors external to the consortium (e.g. the service provider, cloud host)? If yes, are they based inside or outside the EEA, and where?

a) Sensors
b) Wearables
c) Kinect microphone
d) Kinect camera
e) Other technology

13. If the above answer is yes, what kind of mitigation measures can you adopt to protect the personal data of TeNDER patients?

a) Use a comparable technology that does not involve transfer of data to other jurisdictions
b) Opt-out of data sharing with service provider
c) Use the device offline/without internet connection
d) Do not use real names

e) Do not use real birthdates
f) Do not connect to social media profile(s)
g) Use a dedicated email address
h) Use a dedicated device
i) Other measure(s), namely:

1.3 Privacy

14. In order to minimise the impact on privacy, can the use of the technology be limited to a specific time or place, e.g. it can be turned off by the patient?

15. When the service is provided by an external entity (not part of the consortium), is opting out of data sharing possible? If yes, how? Can it easily be done by the patient?

16. If opt-out is not possible, can you use other measures e.g. dedicated emails, dedicated devices, etc.?

a) Opt-out of data sharing with service provider
b) Use the device offline/without internet connection
c) Do not use real names
d) Do not use real birthdates
e) Do not connect to social media profile(s)
f) Use a dedicated email address
g) Use a dedicated device
h) Other measure(s), namely:

17. How can the privacy of third parties, e.g. visitors or other staff be protected, while they are in the same area as the patient involved in TeNDER?

1.3 Socio-ethical aspects

18. What do you think will be the claimed benefit for the user of the technology and general society, regarding the second wave of pilots?

19. Are there any safety risks for the users related to the use of the technology in the second wave?

20. What kind of skills, training and information will be needed for the end-users of this technology?

21. What technical measures might be implemented to assist end-users in a better and faster understanding the technology? What measures can be taken to ensure the right and efficient use of the technology?

22. What other measures could be taken to increase trust of society and individuals in the use of the technology?

1.4 Development of medical technology

23. Will technology be developed that monitors the health status of end-users? If yes, in what way?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

24. Will technology be used that monitors the health status of end-users? If yes, in what way?

a) Fall detection tool
b) Emotion detection tool

c) Recommender

25. Does the technology help prevent, diagnose or provide a prognosis of an illness, injury or disability? If yes, how?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

26. Does the technology send data to health care providers to monitor an illness, injury or disability? If yes, how?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

27. Does the technology suggest some type of treatment or provide some type of alleviation for an illness, injury or disability? If yes, how?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

28. Will the technology used in the second wave be used for any of the following purposes: diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of AD, PD or CVD? If yes, how?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

29. Upon receiving the recommendation from technology, will the decision to diagnose, prevent, monitor, etc. be taken by a human caretaker, or by the technology itself? What is the role of the caretaker in the decision-making process?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

30. Will you use any technology marked with CE and if so, which technology(-ies)?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

31. Do you plan to adopt the CE marking for the technology used in the second wave, and if so, for which technology(-ies)?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

Annex III: Second Impact Assessment – Questionnaire for User Partners

1.1 Questions related to your role in the second wave

1. Are you involving any human participants in the second wave? If yes, how many?

2. Will your organisation use technologies developed by TeNDER partners when you engage human participants during the second wave? If yes, which ones?

e.g. TeNDER app, web interface, HeTRA …

3. Will your organisation use any other existing technologies when you engage human participants during the second wave? If yes, which ones?

e.g. wearables, Kinect camera/microphone

4. Will your organisation process personal data during the TeNDER project? If so, what types of data?

Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, erasure or destruction. For more details on the terms 'personal data' and 'processing', please see D1.1 (section 4.3.3.1). For examples of categories of data please see question 8. Where possible, please separate this with respect to the relevant technologies and other data collecting methods (e.g. xx data is collected with xx sensor, xx data will be collected with questionnaires).

5. Will you cooperate with organisations or entities, external to the project, for processing of the personal data during the second wave? If yes, in which context and for what purpose?

1.2 Data protection

6. What types of data will be collected and processed by the TeNDER system?
Where possible, please separate this with respect to the relevant technologies and other data collecting methods (e.g. xx data is collected with xx sensor, xx component will process xx data). The categories below are provided as an example.

a. Identification data (e.g. name, last name, data of birth, age, gender, email, phone)
b. Personal features
c. Financial data
d. Physical, physiological or behavioural characteristics of a natural person, allowing or confirming their unique identification (please specify)
e. Genetic data
f. Biometric data
g. Other information regarding health, incl. mental health
h. Habits
i. Family composition
j. Hobbies and interests
k. Consumption patterns
l. Residence or home address
m. Education
n. Occupation and employment
o. Social security number
p. Racial or ethnic background
q. Philosophical or spiritual orientation
r. Information on sexual preferences
s. Political orientation or opinion
t. Membership of trade union or affiliation
u. Other memberships
v. Video footage
w. Other, namely:

If possible, fill in the planned collection/processing of data by technology, and specify method of collection/processing:

a) Sensors
b) Wearables
c) Kinect microphone
d) Kinect camera
e) Other technology

7. Whose personal data is being processed?
Please describe the data subjects, i.e. the (groups of) individuals whose personal data will be collected and processed.

8. What is the legal basis for processing of personal data?

9. If the data is collected on the legal basis of consent of the data subject, how do you guarantee that the consent is informed, specific and freely given?

10. Describe the flow of personal data in the second wave (i.e. the route from the data from recording until deletion) and how it will be used.

Please describe briefly the datasets of personal data, the information flows (i.e. what data is collected, where did it come from, where does it go) and the use of all categories of personal data.

11. What is the purpose of processing the data and what are the expected benefits?

12. How long will the personal data be retained? What will happen with the personal data after the second wave? Please define per technology, where possible.

a) Sensors
b) Wearables
c) Kinect microphone
d) Kinect camera
e) Other technology

13. Within your organisation, who apart from the researchers involved in TeNDER could have access to the patient data?

14. What is the scale of the processing in the second wave?

Please give the approximate number of research participants engaged and/or personal data/datasets you hope to collect or need to use?

15. Does the technology being used transfer any data to actors external to the consortium (e.g. the service provider, cloud host)? If yes, are they based inside or outside the EEA, and where?

a) Sensors
b) Wearables
c) Kinect microphone
d) Kinect camera
e) Other technology

16. If the above answer is yes, what kind of mitigation measures can you adopt to protect the personal data of TeNDER patients?

a) Use a comparable technology that does not involve transfer of data to other jurisdictions
b) Opt-out of data sharing with service provider
c) Use the device offline/without internet connection
d) Do not use real names
e) Do not use real birthdates
f) Do not connect to social media profile(s)
g) Use a dedicated email address
h) Use a dedicated device
i) Other measure(s), namely:

1.3 Privacy

17. In order to minimise the impact on privacy, can the use of the technology be limited to a specific time or place, e.g. it can be turned off by the patient?

18. When the service is provided by an external entity (not part of the consortium), is opting out of data sharing possible? If yes, how? Can it easily be done by the patient?

19. If opt-out is not possible, can you use other measures e.g. dedicated emails, dedicated devices, etc.?

a) Opt-out of data sharing with service provider

b) Use the device offline/without internet connection
c) Do not use real names
d) Do not use real birthdates
e) Do not connect to social media profile(s)
f) Use a dedicated email address
g) Use a dedicated device
h) Other measure(s), namely:

20. How can the privacy of third parties, e.g. visitors or other staff be protected, while they are in the same area as the participant(s) involved in TeNDER?

1.3 Socio-ethical aspects

21. What do you think will be the claimed benefit for the user of the technology and general society, regarding the second wave of pilots?

22. Are there any safety risks for the users related to the use of the technology in the second wave?

23. What kind of skills, training and information will be needed for the end-users of this technology?

24. What technical measures might be implemented to assist end-users in a better and faster understanding the technology? What measures can be taken to ensure the right and efficient use of the technology?

25. What other measures could be taken to increase trust of society and individuals in the use of the technology?

1.4 Development of medical technology

26. Will technology be developed that monitors the health status of end-users? If yes, in what way?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

27. Will technology be used that monitors the health status of end-users? If yes, in what way?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

28. Does the technology help prevent, diagnose or provide a prognosis of an illness, injury or disability? If yes, how?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

29. Does the technology send data to health care providers to monitor an illness, injury or disability? If yes, how?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

30. Does the technology suggest some type of treatment or provide some type of alleviation for an illness, injury or disability? If yes, how?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

31. Will the technology used in the second wave be used for any of the following purposes: diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of AD, PD or CVD? If yes, how?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

32. Upon receiving the recommendation from technology, will the decision to diagnose, prevent, monitor, etc. be taken by a human caretaker, or by the technology itself? What is the role of the caretaker in the decision-making process?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

33. Will you use any technology marked with CE and if so, which technology(-ies)?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

34. Do you plan to adopt the CE marking for the technology used in the second wave, and if so, for which technology(-ies)?

a) Fall detection tool
b) Emotion detection tool
c) Recommender

Annex IV: Third Impact Assessment – Questionnaire for Coordinating Tech Partners

1.1 Questions related to your role in the third wave

1. Will your organisation develop any technology (or component) for the third wave or contribute thereto?

If yes, please name and describe it.

2. Will your organisation use any existing technology for the third wave?
   If yes, please name and describe it and the purpose of its use. Also specify the source of the technology (own, another TeNDER partner or external tech provider-which one).

3. Will your organisation process or intend to process personal data on behalf of the data controlling partners in the TeNDER consortium in the context of the third wave? If so, what types of data?
   Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, erasure or destruction. This includes the processing of pseudonymised data. For more details on the terms 'personal data' and 'processing', please see D1.1 (section 4.3.3.1). For examples of categories of data please see question 4.

1.2 Data protection

4. What types of data will be collected and processed by the TeNDER system?
Where possible, please separate this with respect to the relevant technologies and other data collecting methods (e.g. xx data is collected with xx sensor, xx component will process xx data). The categories below are provided as an example.

a. Identification data (e.g. name, last name, data of birth, age, gender, email, phone)
b. Personal features
c. Financial data
d. Physical, physiological or behavioural characteristics of a natural person, allowing or confirming their unique identification (please specify)
e. Genetic data
f. Biometric data
g. Other information regarding health, incl. mental health
h. Habits
i. Family composition
j. Hobbies and interests
k. Consumption patterns
l. Residence or home address
m. Education
n. Occupation and employment
o. Social security number
p. Racial or ethnic background
q. Philosophical or spiritual orientation
r. Information on sexual preferences
s. Political orientation or opinion
t. Membership of trade union or affiliation
u. Other memberships
v. Video footage
w. Other, namely:

If possible, fill in the planned collection/processing of data by technology, and specify method of collection/processing.

If possible, please also include information per profile (admin, caregiver, patient, physician etc.).

a) Recommender
b) Social communication
c) Virtual assistant
d) Other functionalities

5. Whose personal data is being processed?
Please describe the data subjects, i.e. the (groups of) individuals whose personal data will be collected and processed.

6. What is the legal basis for processing of personal data?

7. What is the purpose of processing the data and what are the expected benefits?

a) Recommender
b) Social communication
c) Virtual assistant
d) Other functionalities

8. How long will the personal data be retained? What will happen with the personal data after the third wave? Please define per technology, where possible.

a) Recommender
b) Social communication
c) Virtual assistant
d) Other functionalities

9. What kind of security measures will you take to ensure security of personal data? Please define per technology, where possible.

a) Recommender
b) Social communication
c) Virtual assistant
d) Other functionalities

10. How will data gathered in the functionalities being tested contribute to development of:

- Recommender

	TeNDER app	Questionnaires
Which data will be extracted?		

Will a patient profile be built?		
What kind of decision will this functionality suggest, if any?		

- Social communication

	TeNDER app	Questionnaires
Which data will be extracted?		
Will a patient profile be built?		
What kind of decision will this functionality suggest, if any?		

- Virtual assistant

	TeNDER app	Questionnaires
Which data will be extracted?		
Will a patient profile be built?		
What kind of decision will this functionality suggest, if any?		

- Other functionalities

	TeNDER app	Questionnaires
Which data will be extracted?		
Will a patient profile be built?		
What kind of decision will this functionality suggest, if any?		

11. Upon receiving the recommendation from technology, will the decision to take an action be taken by the patient, or by the technology itself? What is the role of the patient in the decision-making process?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

12. Is the processing of personal data really necessary to achieve the purpose identified above? Would other means (mock data, anonymous data set, fewer variables of personal data) be less satisfactory to achieve the same outcome? Please specify per technology:

a) Recommender
b) Social communication
c) Virtual assistant
d) Other functionalities

13. Does the technology being used transfer any data to actors external to the consortium (e.g. the service provider, cloud host)? If yes, are they based inside or outside the EEA, and where?

a) Recommender
b) Social communication
c) Virtual assistant
d) Other functionalities

14. If the above answer is yes, what kind of mitigation measures can you adopt to protect the personal data of TeNDER patients?

a) Use a comparable technology that does not involve transfer of data to other jurisdictions
b) Opt-out of data sharing with service provider
c) Use the device offline/without internet connection
d) Do not use real names
e) Do not use real birthdates
f) Do not connect to social media profile(s)
g) Use a dedicated email address
h) Use a dedicated device
i) Other measure(s), namely:

1.3 Privacy

15. In order to minimise the impact on privacy, can the use of the technology be limited to a specific time or place, e.g. it can be turned off by the patient?

16. When the service is provided by an external entity (not part of the consortium), is opting out of data sharing possible? If yes, how? Can it easily be done by the patient?

17. If opt-out is not possible, can you use other measures e.g. dedicated emails, dedicated devices, etc.?

a) Opt-out of data sharing with service provider
b) Use the device offline/without internet connection
c) Do not use real names
d) Do not use real birthdates
e) Do not connect to social media profile(s)
f) Use a dedicated email address
g) Use a dedicated device
h) Other measure(s), namely:

18. How can the privacy of third parties, e.g. visitors or other staff be protected, while they are in the same area as the patient involved in TeNDER?

1.3 Socio-ethical aspects

19. What do you think will be the claimed benefit for the user of the technology and general society, regarding the third wave of pilots?

20. Are there any safety risks for the users related to the use of the technology in the third wave?

21. What kind of skills, training and information will be needed for the end-users of this technology?

22. What technical measures might be implemented to assist end-users in a better and faster understanding the technology? What measures can be taken to ensure the right and efficient use of the technology?

23. What other measures could be taken to increase trust of society and individuals in the use of the technology?

1.4 Development of medical technology

24. Will technology be developed that monitors the health status of end-users? If yes, in what way?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

25. Will technology be used that monitors the health status of end-users? If yes, in what way?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

26. Does the technology help prevent, diagnose or provide a prognosis of an illness, injury or disability? If yes, how?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

27. Does the technology send data to health care providers to monitor an illness, injury or disability? If yes, how?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

28. Does the technology suggest some type of treatment or provide some type of alleviation for an illness, injury or disability? If yes, how?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

29. Will the technology used in the third wave be used for any of the following purposes: diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of AD, PD or CVD? If yes, how?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

30. Upon receiving the recommendation from technology, will the decision to diagnose, prevent, monitor, etc. be taken by a human caretaker, or by the technology itself? What is the role of the caretaker in the decision-making process?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

31. Will you use any technology marked with CE and if so, which technology(-ies)?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

32. Do you plan to adopt the CE marking for the technology used in the third wave, and if so, for which technology(-ies)?

a. Recommender

b. Social communication
c. Virtual assistant
d. Other functionalities

Annex V: Third Impact Assessment – Questionnaire for Tech Partners

1.1 Questions related to your role in the third wave

1. Will your organisation develop any technology (or component) for the third wave or contribute thereto?

If yes, please name and describe it.

2. Will your organisation use any existing technology for the third wave?
If yes, please name and describe it and the purpose of its use. Also specify the source of the technology.

3. Will your organisation process or intend to process personal data on behalf of the data controlling partners in the TeNDER consortium in the context of the third wave? If so, what types of data?
Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, erasure or destruction. This includes the processing of pseudonymised data. For more details on the terms 'personal data' and 'processing', please see D1.1 (section 4.3.3.1). For examples of categories of data please see question 4.

1.2 Data protection

4. What types of data will be collected and processed by the TeNDER system?
Where possible, please separate this with respect to the relevant technologies and other data collecting methods (e.g. xx data is collected with xx sensor, xx component will process xx data). The categories below are provided as an example.

a. Identification data (e.g. name, last name, data of birth, age, gender, email, phone)
b. Personal features
c. Financial data
j. Hobbies and interests
k. Consumption patterns
l. Residence or home address
m. Education
n. Occupation and employment

d. Physical, physiological or behavioural characteristics of a natural person, allowing or confirming their unique identification (please specify)
e. Genetic data
f. Biometric data
g. Other information regarding health, incl. mental health
h. Habits
i. Family composition
o. Social security number
p. Racial or ethnic background
q. Philosophical or spiritual orientation
r. Information on sexual preferences
s. Political orientation or opinion
t. Membership of trade union or affiliation
u. Other memberships
v. Video footage
w. Other, namely:

If possible, fill in the planned collection/processing of data by technology, and specify method of collection/processing:

a) Recommender
b) Social communication
c) Virtual assistant
d) Other functionalities

5. Whose personal data is being processed?
Please describe the data subjects, i.e. the (groups of) individuals whose personal data will be collected and processed.

6. What is the legal basis for processing of personal data?

7. What is the purpose of processing the data and what are the expected benefits?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

8. How long will the personal data be retained? What will happen with the personal data afterwards?

a. Recommender b. Social communication c. Virtual assistant d. Other functionalities

9. What kind of security measures will you take to ensure security of personal data?

a. Recommender b. Social communication c. Virtual assistant d. Other functionalities

10. How will data gathered in the tested functionalities be used for:

- Recommender

	TeNDER app	Questionnaires
Which data will be extracted?		
Will a patient profile be built?		
What kind of decision will this functionality suggest, if any?		

- Social communication

	TeNDER app	Questionnaires
Which data will be extracted?		
Will a patient profile be built?		
What kind of decision will this functionality suggest, if any?		

- Virtual assistant

	TeNDER app	Questionnaires
Which data will be extracted?		
Will a patient profile be built?		
What kind of decision will this functionality suggest, if any?		

- Other functionalities

	TeNDER app	Questionnaires
Which data will be extracted?		
Will a patient profile be built?		
What kind of decision will this functionality suggest, if any?		

11. Upon receiving the recommendation from technology, will the decision to take an action be taken by the patient, or by the technology itself? What is the role of the patient in the decision-making process?

a. Recommender
b. Social communications
c. Virtual assistant
d. Other functionalities

12. Is the processing of personal data really necessary to achieve the purpose identified above? Would other means (mock data, anonymous data set, fewer variables of personal data) be less satisfactory to achieve the same outcome? Please specify per technology:

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

13. Does the technology being used transfer any data to actors external to the consortium (e.g. the service provider, cloud host)? If yes, are they based inside or outside the EEA, and where?

a. Recommender b. Social communication c. Virtual assistant d. Other functionalities

14. If the above answer is yes, what kind of mitigation measures can you adopt to protect the personal data of TeNDER patients?

a) Use a comparable technology that does not involve transfer of data to other jurisdictions b) Opt-out of data sharing with service provider c) Use the device offline/without internet connection d) Do not use real names e) Do not use real birthdates f) Do not connect to social media profile(s) g) Use a dedicated email address h) Use a dedicated device i) Other measure(s), namely:

1.3 Privacy

15. In order to minimise the impact on privacy, can the use of the technology be limited to a specific time or place, e.g. it can be turned off by the patient?

16. When the service is provided by an external entity (not part of the consortium), is opting out of data sharing possible? If yes, how? Can it easily be done by the patient?

17. If opt-out is not possible, can you use other measures e.g. dedicated emails, dedicated devices, etc.?

a) Opt-out of data sharing with service provider

b) Use the device offline/without internet connection
c) Do not use real names
d) Do not use real birthdates
e) Do not connect to social media profile(s)
f) Use a dedicated email address
g) Use a dedicated device
h) Other measure(s), namely:

18. How can the privacy of third parties, e.g. visitors or other staff be protected, while they are in the same area as the patient involved in TeNDER?

1.3 Socio-ethical aspects

19. What do you think will be the claimed benefit for the user of the technology and general society, regarding the third wave of pilots?

20. Are there any safety risks for the users related to the use of the technology in the third wave?

21. What kind of skills, training and information will be needed for the end-users of this technology?

22. What technical measures might be implemented to assist end-users in a better and faster understanding the technology? What measures can be taken to ensure the right and efficient use of the technology?

23. What other measures could be taken to increase trust of society and individuals in the use of the technology?

1.4 Development of medical technology

24. Will technology be developed that monitors the health status of end-users? If yes, in what way?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

25. Will technology be used that monitors the health status of end-users? If yes, in what way?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

26. Does the technology help prevent, diagnose or provide a prognosis of an illness, injury or disability? If yes, how?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

27. Does the technology send data to health care providers to monitor an illness, injury or disability? If yes, how?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

28. Does the technology suggest some type of treatment or provide some type of alleviation for an illness, injury or disability? If yes, how?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

29. Will the technology used in the third wave be used for any of the following purposes: diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of AD, PD or CVD? If yes, how?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

30. Upon receiving the recommendation from technology, will the decision to diagnose, prevent, monitor, etc. be taken by a human caretaker, or by the technology itself? What is the role of the caretaker in the decision-making process?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

31. Will you use any technology marked with CE and if so, which technology(-ies)?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

32. Do you plan to adopt the CE marking for the technology used in the third wave, and if so, for which technology(-ies)?

a. Recommender
b. Social communication
c. Virtual assistant
d. Other functionalities

Annex VI: Third Impact Assessment – Questionnaire for User Partners

1.1 Questions related to your role in the third wave

1. Are you involving any human participants in the third wave? If yes, how many?

2. Will your organisation use technologies developed by TeNDER partners when you engage human participants during the third wave? If yes, which ones?

e.g. TeNDER app, web interface, HeTRA …

3. Will your organisation use any other existing technologies when you engage human participants during the third wave? If yes, which ones?

e.g. wearables, Kinect camera/microphone

4. Will your organisation process personal data during the TeNDER project? If so, what types of data?

Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, erasure or destruction. For more details on the terms 'personal data' and 'processing', please see D1.1 (section 4.3.3.1). For examples of categories of data please see question 8. Where possible, please separate this with respect to the relevant technologies and other data collecting methods (e.g. xx data is collected with xx sensor, xx data will be collected with questionnaires).

5. Will you cooperate with organisations or entities, external to the project, for processing of the personal data during the third wave? If yes, in which context and for what purpose?

1.2 Data protection

6. What types of data will be collected and processed by the TeNDER system?
Where possible, please separate this with respect to the relevant technologies and other data collecting methods (e.g. xx data is collected with xx sensor, xx component will process xx data). The categories below are provided as an example.

x. Identification data (e.g. name, last name, data of birth, age, gender, email, phone)
y. Personal features
z. Financial data
aa. Physical, physiological or behavioural characteristics of a natural person, allowing or confirming their unique identification (please specify)
bb. Genetic data
cc. Biometric data
dd. Other information regarding health, incl. mental health
ee. Habits
ff. Family composition
gg. Hobbies and interests
hh. Consumption patterns
ii. Residence or home address
jj. Education
kk. Occupation and employment
ll. Social security number
mm. Racial or ethnic background
nn. Philosophical or spiritual orientation
oo. Information on sexual preferences
pp. Political orientation or opinion
qq. Membership of trade union or affiliation
rr. Other memberships
ss. Video footage
tt. Other, namely:

If possible, fill in the planned collection/processing of data by technology, and specify method of collection/processing.

If possible, please also include information per profile (admin, caregiver, patient, physician etc.).

a. User interface – admin profile
b. Web app
c. Mobile app
d. Virtual assistant

7. Whose personal data is being processed?
Please describe the data subjects, i.e. the (groups of) individuals whose personal data will be collected and processed.

8. What is the legal basis for processing of personal data?

9. If the data is collected on the legal basis of consent of the data subject, how do you guarantee that the consent is informed, specific and freely given?

10. Describe the flow of personal data in the third wave (i.e. the route from the data from recording until deletion) and how it will be used.

Please describe briefly the datasets of personal data, the information flows (i.e. what data is collected, where did it come from, where does it go) and the use of all categories of personal data.

11. Upon receiving the recommendation from technology, will the decision to take an action be taken by the patient, or by the technology itself? What is the role of the patient in the decision-making process?

a. User interface – admin profile
b. Web app
c. Mobile app
d. Virtual assistant

12. What is the purpose of processing the data and what are the expected benefits?

13. How long will the personal data be retained? What will happen with the personal data after the third wave? Please define per technology, where possible.

a. User interface – admin profile
b. Web app
c. Mobile app
d. Virtual assistant

14. Within your organisation, who apart from the researchers involved in TeNDER could have access to the patient data?

15. What is the scale of the processing in the third wave?

Please give the approximate number of research participants engaged and/or personal data/datasets you hope to collect or need to use?

16. Does the technology being used transfer any data to actors external to the consortium (e.g. the service provider, cloud host)? If yes, are they based inside or outside the EEA, and where?

a. User interface – admin profile
b. Web app
c. Mobile app
d. Virtual assistant

17. If the above answer is yes, what kind of mitigation measures can you adopt to protect the personal data of TeNDER patients?

a) Use a comparable technology that does not involve transfer of data to other jurisdictions
b) Opt-out of data sharing with service provider
c) Use the device offline/without internet connection
d) Do not use real names
e) Do not use real birthdates
f) Do not connect to social media profile(s)
g) Use a dedicated email address
h) Use a dedicated device
i) Other measure(s), namely:

1.3 Privacy

18. In order to minimise the impact on privacy, can the use of the technology be limited to a specific time or place, e.g. it can be turned off by the patient?

19. When the service is provided by an external entity (not part of the consortium), is opting out of data sharing possible? If yes, how? Can it easily be done by the patient?

20. If opt-out is not possible, can you use other measures e.g. dedicated emails, dedicated devices, etc.?

a) Opt-out of data sharing with service provider b) Use the device offline/without internet connection c) Do not use real names d) Do not use real birthdates e) Do not connect to social media profile(s) f) Use a dedicated email address g) Use a dedicated device h) Other measure(s), namely:

21. How can the privacy of third parties, e.g. visitors or other staff be protected, while they are in the same area as the participant(s) involved in TeNDER?

1.3 Socio-ethical aspects

22. What do you think will be the claimed benefit for the user of the technology and general society, regarding the third wave of pilots?

23. Are there any safety risks for the users related to the use of the technology in the third wave?

24. What kind of skills, training and information will be needed for the end-users of this technology?

25. What technical measures might be implemented to assist end-users in a better and faster understanding the technology? What measures can be taken to ensure the right and efficient use of the technology?

26. What other measures could be taken to increase trust of society and individuals in the use of the technology?

1.4 Development of medical technology

27. Will technology be developed that monitors the health status of end-users? If yes, in what way?

a. User interface – admin profile
b. Web app
c. Mobile app
d. Virtual assistant

28. Will technology be used that monitors the health status of end-users? If yes, in what way?

a. User interface – admin profile
b. Web app
c. Mobile app
d. Virtual assistant

29. Does the technology help prevent, diagnose or provide a prognosis of an illness, injury or disability? If yes, how?

a. User interface – admin profile
b. Web app
c. Mobile app
d. Virtual assistant

30. Does the technology send data to health care providers to monitor an illness, injury or disability? If yes, how?

a. User interface – admin profile
b. Web app
c. Mobile app

d. Virtual assistant

31. Does the technology suggest some type of treatment or provide some type of alleviation for an illness, injury or disability? If yes, how?

a. User interface – admin profile
b. Web app
c. Mobile app
d. Virtual assistant

32. Will the technology used in the third wave be used for any of the following purposes: diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of AD, PD or CVD? If yes, how?

a. User interface – admin profile
b. Web app
c. Mobile app
d. Virtual assistant

33. Upon receiving the recommendation from technology, will the decision to diagnose, prevent, monitor, etc. be taken by a human caretaker, or by the technology itself? What is the role of the caretaker in the decision-making process?

a. User interface – admin profile
b. Web app
c. Mobile app
d. Virtual assistant

34. Will you use any technology marked with CE and if so, which technology(-ies)?

a. User interface – admin profile
b. Web app
c. Mobile app
d. Virtual assistant

35. Do you plan to adopt the CE marking for the technology used in the third wave, and if so, for which technology(-ies)?

a. User interface – admin profile
b. Web app
c. Mobile app
d. Virtual assistant