



CAPABLE

Cancer Patients Better Life Experience

Grant Agreement No. 875052
Start Date: 01/01/2020 (48 Months)

Deliverable No. 7.6 **Informed Patient Consent/Assent Form, Ethical Committee Approval, Training Materials, and Technical Manual for Maintenance**

Due Date: [31/12/2022]
Submitted On: [30/12/2022]
Resubmitted On: [15/08/2023]

Coordinator	University of Pavia (UNIPV)
Deliverable Lead Partner	University of Pavia (UNIPV)
Contributing Partners	
Contact	Prof. Silvana Quaglini
Email	silvana.quaglini@unipv.it
Website	www.capable-project.eu

Deliverable Type		
R	Document, report	
DEM	Demonstrator, pilot, prototype	[X]
DEC	Websites, patent fillings, videos etc.	
OTHER		
Dissemination Level		
PU	Public	[X]
CO	Confidential (Consortium members including the Commission Services)	
CI	Classified Information (Commission Decision 2015/444/EC)	

Table of Contents

Glossary	3
Versions History	4
1. Executive Summary	5
2. Informed Patient Consent Form and Ethical Committee Approval	6
Roadmap to the CAPABLE pilot study	6
3. Training plan and materials	9
Training plan	9
Training materials	11
4. Technical Maintenance	12
Regular maintenance of the CAPABLE components	12
Issues management	17
5. Conclusions	20
6. Annexes	21
Section 2	21
Section 3	22

List of Figures

Figure 1: Roadmap to the CAPABLE pilot studies 7

Glossary

API - Application Programming Interface
CCMO - Central Committee on Research Involving Human Subjects
CIG - Computer Interpretable Guidelines
CM - Case Manager
DP - Data Platform
DPIA - Data Protection Impact Assessments
DPO - Data Protection Officer
DSS - Decision Support System
DTA - Data Transfer Agreements
FHIR - Fast Healthcare Interoperability Resources
GDPR - General Data Protection Regulation
GoCom - Goal-based Comorbidity
GUI - Graphical User Interface
HAPI - High Level API
HL7 - Health Level Seven
HTTP - Hypertext Transfer Protocol
ICSM - Istituti Clinici Scientifici Maugeri
IT - Information Technology
KDOM - Knowledge-Data Ontology Mapper
LAN - Local Area Network
MDM - Mobile Device Manager
MDR - Medical Device Regulation
NKI - Netherlands Cancer Institute
OS - Operating System
PDSS - Physician Decision Support System
REST - REpresentational State Transfer
RxNav - RxNorm Navigator
SLF4J - Simple Logging Facade for Java
SOC - Security Operations Center
SQL - Structured Query Language
TF1 - Task Force One
UNIPV - Università degli Studi di Pavia
VC - Virtual Coach
VM - Virtual Machine
VPN - Virtual Private Network

Versions History

Version	Date	Author	Comments
1.0	30/11/2022	Lucia Sacchi, UNIPV Valentina Tibollo, ICSM	First version
1.1	20/12/2022	Mor Peleg, UoH	Internal Review
1.2	28/12/2022	Silvana Quaglini, UNIPV	Final review
1.3	03/07/2023	Lucia Sacchi, UNIPV Valentina Tibollo, ICSM Sara Azzini, UNIPV	Revision after ethics check
	15/08/2023	UNIPV team by Lucia Sacchi	Updated per Commission's request for clarification

1. Executive Summary

In this deliverable we present the activities carried out in WP7 in preparation for the CAPABLE pilot studies. These activities include: i) the preparation of the preliminary documentation for **study authorization** in compliance to the current EU regulations in terms of **data protection and medical devices usage**, ii) the preparation of a **training plan** for the users of the system and for the technical staff who will support users during the study, and (iii) the **definition of the policies for maintenance** of the CAPABLE software and of the devices that are needed for it to be used. This document is organized in three Sections, each one related to the described activities. Being this a Demonstration deliverable, it includes the references to all the documentation that has been prepared during the last year of the project, which is shared through links to files shared on Google Drive. The links to the available documentation are reported in the Annexes Section.

2. Informed Patient Consent Form and Ethical Committee Approval

Roadmap to the CAPABLE pilot study

During Year 3 of the project, the activities of WP7 have been focused on the set up of the clinical studies, to comply with all the regulatory procedures and to the requirements of each hospital.

Since the CAPABLE system is a software that deals with the processing of health-related data, it has to comply with General Data Protection Regulation (GDPR) and Medical Device Regulation (MDR). In addition, since the pilot study involves human subjects, an approval by the Ethical Committees is mandatory.

According to Article 35 of the GDPR, a Data Protection Impact Assessments (DPIA) is required as part of the *protection by design* principle, since the type of processing performed by the CAPABLE system involves new technologies and personal data: “racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation”. One of the requirements of the DPIA is the definition of the roles and responsibilities of all the parties involved in the data processing. For the CAPABLE study, together with the Data Protection Officers (DPOs) of the hospitals, we identified the following roles: the hospitals responsible for running the clinical study act as Data Controller, whereas the project partners are appointed as Data Processors.

According to Article 62 of the Medical Device Regulation (MDR), CAPABLE clinical investigation has the purpose to “establish and verify the clinical benefits of a device as specified by its manufacturer”. Since the CAPABLE system is classified as a class IIa medical device without CE marking, the clinical investigation must undergo an authorization process in each country where it is carried out. This procedure is specified in

Informed patient consent/assent form, ethical committee approval, training materials, and technical manual for maintenance [D7.6]

the MDR and requires similar documentation both in Italy and in the Netherlands. For Italy, this is the link with the instructions for the procedure:

<https://www.salute.gov.it/portale/moduliServizi/dettaglioSchedaModuliServizi.jsp?lingua=italiano&label=servizionline&idMat=DM&idAmb=SC&idSrv=PRE1&flag=P>.

For the Netherlands the procedure can be found here:

<https://english.ccmo.nl/investigators/clinical-investigations-with-medical-devices/standard-research-file-medical-devices>

To comply with the requirements described above, we have performed the following steps, as illustrated in Figure 1.



Figure 1 - Roadmap to the CAPABLE pilot studies

1. Preparation of the DPIA

For each data processing site, one DPIA document was prepared and signed by the Data Controller. The document includes a technical description of the CAPABLE system and of the data flow, the description of all the data processing involved, the roles and responsibilities of the parties involved, and a description and assessment of risks and measures to mitigate them. According to the decision to appoint partners as Data Processors, Data Transfer Agreements (DTA) were prepared and signed by the legal representatives of each institution. To be eligible as a Data Processor, each partner had to fill in and sign a Security Checklist about the security measures available at its institution.

2. Preparation of the Ethical Committee documentation

After finalizing the DPIA, the next step was the preparation of the documentation needed for Ethical Committee approval. The main documents requested by the Ethical Committees of the hospitals are: the clinical protocol, the informed consent, the privacy statement, and the DPIA. Ethical Committee approval was obtained in

Informed patient consent/assent form, ethical committee approval, training materials, and technical manual for maintenance [D7.6]

ICSM on 11/05/2022 (amended on 21/02/2023), in NKI on 28/12/2022 and in Bari on 22/02/2023.

3. Preparation of the submission for the Medical Device Registration

To be able to submit the documentation for authorization to the clinical investigation according to MDR, the Italian procedure requests a preliminary approval by the Ethical Committee. The documentation is then submitted to the Italian Ministry of Health. In the Netherlands, the documentation must be submitted to the Central Committee on Research Involving Human Subjects (CCMO). CCMO approval is needed to proceed to the Ethical Committee submission.

For Italy, the documentation was submitted in Month 35 and, after several iterations, we received the validation of the request on March 29th 2023. For the Netherlands, the CCMO approved the documentation on 21/11/2022.

The links to the prepared documentations are reported in the Annexes section.

3. Training plan and materials

Training plan

The training plan for the CAPABLE study consists of a set of activities that involve the users (patients and healthcare professionals) and the technical/research staff at the hospitals.

Training plan for technical/research staff

For the technical/research staff, the training activities have started at Month 30, after the release of the first prototypes of the mobile app and the physician dashboard.

In ICSM and in Bari, two biomedical engineers will be responsible for following the study from a technical point of view. In particular, they will act as *contact points* both for patients and healthcare professionals. In NKI the study coordinator (PhD student with epidemiology background) will be the contact point for patients and healthcare professionals. The role of the contact point involves the preparation of the devices for the enrollment and technical support during all the study phases (enrollment, observation period, and end of the study). In NKI, technical backup will be retrieved from the technical team by the study coordinator when necessary.

The preparation of the devices includes the following activities:

- check if the personal smartphone of the patient is compliant with the technical requirements of the CAPABLE system, and, if so, check if the patient is willing to use it for the study and install the CAPABLE app on the smartphone;
- In case the previous conditions are not met, prepare a dedicated smartphone to be given to the patient. The preparation of the smartphone consists of: update the smartphone to the latest Android version, configure a dedicated Google account (using an email address not able to identify the patient, such as capable.test2022.X@gmail.com), set a security PIN to protect the device, provide the smartphone with a prepaid data SIM card, install the CAPABLE app;
- install the HealthConnect Asus app and OmnicareHub Asus app on the smartphone that will be used for the study. Create an Asus account for the patient and couple the smartwatch to the smartphone via Bluetooth.

The technical support during the study phases includes the following activities:

- enrollment: delivery of the devices to the patient and training on the devices' main functionalities; support to the healthcare professionals during enrollment;
- observation period: tracking of all the issues/bugs reported by the users during the CAPABLE study. If possible, management of the issue and direct feedback to the users, otherwise report the issue to the CAPABLE partner responsible for solving it, inform the users of the next steps related to the issue management or solution;
- end of the study: collection of the devices, download of the usage data, uninstallation of the CAPABLE app in case of usage of personal smartphone, factory reset of the smartphone in case one was provided to the patient.

Given these activities, the training for the technical/research staff started in Month 28, when a final decision was taken on the type of the devices to be bought and the first purchases were done. UNIPV staff was responsible for the initial training of ICSM technical staff, which was completed in Month 34. After one month of internal testing of the devices performed by ICSM technical staff, in Month 36 UNIPV and ICSM have started the training procedures for the research/technical staff at NKI and Bari.

The activities performed during the training are aimed at getting experience on:

- managing the configuration and use of the devices (smartwatches and smartphones purchased)
- the functionalities of the CAPABLE patient app and how to use it
- the functionalities of the CAPABLE physician dashboard and how to use it
- knowledge of the clinical study workflow, from the enrollment to the end of the study, and the involved healthcare professionals
- knowledge of the CAPABLE system components and architecture, in order to identify the partner involved in the solution of possible issues
- managing procedures for malfunctioning and bugs
- knowledge on how to train users in preparation for the clinical study
- knowledge on the maintenance plan

Training plan for healthcare professionals

The healthcare professionals involved in the CAPABLE study are oncologists, nutritionists and clinical psychologists. All of them follow the same training plan. During the study, they will be responsible for identifying patients matching inclusion criteria, presenting the CAPABLE project and ask for intention to participate, enroll the patient in the system, follow the patient during the study through the CAPABLE physician dashboard (in addition to the regular control visits) and support the patient for possible issues related to the use of the system.

The training activities for the healthcare professionals will be devoted to gain experience on:

- CAPABLE project and how to present it to the patients and the caregivers
- knowledge of the clinical study protocol
- knowledge of the material that has to be collected during the study
- the functionalities of the CAPABLE physician dashboard and how to use it
- the functionalities of the CAPABLE patient app and how to use it
- basics on the use of the smartwatch
- knowledge on the technical support workflow, to be able to correctly address patients who might report an issue to the healthcare professional

For the healthcare professionals, a workshop to introduce the functionalities of the CAPABLE system was organized in March 2022 by UNIPV and ICSM. During Month 36, one-on-one training sessions held by UNIPV and ICSM technical staff were organized. Three of these sessions have already been completed in ICSM. Since it is foreseen that in 2023 more healthcare professionals will take part in the study, additional specific one-on-one training sessions will be organized accordingly.

In NKI an initiation visit will be held for all involved doctors and nurse practitioners in Month 37, before enrollment starts. During this visit the endpoints of the study will be explained, and the study population to be included. Furthermore, advice for counseling patients to participate in the study will be given. After the initiation visit, one-on-one 30-minute training sessions will be held with involved healthcare providers, in which we will walk through the CAPABLE dashboard and patient app with support of the instruction guides. Contact persons will be appointed for the healthcare professionals in case of help needed.

Training plan for patients and caregivers

After signing the informed consent and having been enrolled in the CAPABLE system by the oncologist, patients will undergo a personal training session performed by the hospital technical/research staff. If the patient indicates that he wants to involve a caregiver in the study, the caregiver will take part in the training sessions as well.

During the training session, the patient will learn:

- the main objectives of the CAPABLE study, the importance of correctly reporting data and the effort required during the study
- the functionalities of the CAPABLE patient app and how to use it
- using the smartwatch, including synchronization procedures with the Asus Cloud and blood pressure calibration procedures
- managing of the accounts connected to the project (smartphone, Asus and patient app)
- how to identify possible malfunctioning and how to promptly report them through the right communication channels
- how to proceed in case of software updates affecting the devices used in the study

Training materials

Training materials describing the functionalities of the system will be provided to patients and clinicians.

The training materials include:

- user manuals for the clinicians' dashboard (available in English)
- user manuals for the patient app (available in Italian and Dutch and translated in English for WP7 reporting), including also instructions for the smartwatch usage
- appendix to the instructions for use in accordance with Attachment 1, point 23.4 Medical Device Regulation (available in Italian and translated in English)
- video tutorials on the basic functionalities of the patient app (available with English and Italian subtitles)

The links to the available materials are reported in the Annexes section.

4. Technical Maintenance

This section presents the technical maintenance plan of the CAPABLE system during the pilot study. The plan is designed to manage two situations: the regular maintenance of the CAPABLE components during normal functioning, and the management of unexpected issues and possible malfunctioning.

Regular maintenance of the CAPABLE components

In this section we present the regular maintenance plan for each of the CAPABLE components. Regular maintenance activities are aimed at checking the expected behavior and timely detecting possible malfunctioning.

Monitoring the Case Manager

The Case Manager (CM) serves the purpose of notifying all the “knowledgeable” components of the CAPABLE system whenever their events of interest occur. From an *external point of view*, the CM is seen as a REST server, to which both the Data Platform (DP) and the other components connect as REST clients. The DP communicates every newly added Resource so that the CM may verify if their additions, or even their missed additions, trigger some events for any component. The latter regularly connect checking for events while they remain blocked in a long polling connection if none are available. From an *internal point of view*, because of the task it accomplishes, the CM is essentially a scheduler that has some logic always up and running, even when no new Resources are sent by the DP.

This peculiar combination of external and internal standpoints greatly simplifies monitoring. To this aim, the CM maintains a set of rotating logs of a fixed size to which all the major internal activities are written with a customizable level of detail. In particular, analyzing those logs provides reports either on the internal health state of the CM as well as on the health states of any other component connecting through REST. Here is a simplified list of what is collected in the logs:

1. Whenever the main scheduler thread runs, a new record is written in the logs. Since this happens at regular times, defined by the developer, it is easy to tell if something is not going as expected within the CM logic;
2. Whenever a component starts a long polling connection a new record is written in the logs. Components regularly connect to the CM for fetching events with a frequency chosen by their developers. So even though each component should have their internal health monitoring system, the logs maintained by the CM provides an alternative way of detecting faults in the other components;
3. When a new event is generated a new record is stored in the logs. Thus it is quite easy to tell if an event that was generated has not been properly serviced by the components.

Issue (3) clearly requires the combined analysis of the logs generated by the CM and the involved component and should be performed manually. However, analysis of 1) and 2) are managed by automated scripts, looking for any required heartbeat signal and sending messages (i.e. to the console or mail) whenever something is not going as expected.

Monitoring the Data Platform

Data Platform constitutes the CAPABLE system’s persistence layer; it is made by a SQL database (PostgreSQL) accessed through a FHIR-compliant REST layer.

Informed patient consent/assent form, ethical committee approval, training materials, and technical manual for maintenance [D7.6]

Therefore, DP can be monitored at different levels:

- at database level, leveraging the PostgreSQL logs and a special table, called `f_update`, which keeps track of all resources written in the DP associated with date of creation and component responsible for it.
- at web service level, with specific logs keeping track of all operations performed on the component.

Both monitoring activities need access to the Virtual Machine hosting the DP to be established, since no web interface for them has been developed.

Monitoring the Knowledge-Data Ontology Mapper (KDOM)

KDOM provides a log mechanism that exposes: abstraction requests information, abstraction processing data, abstraction results, generated results resources. This log can help the users to monitor KDOM activity.

The log file is based on a plain text format and contains: Date, Time, and Activity. The file can be read by any text reader (e.g., Notepad). To see the log events in real-time KDOM's provides a console manager that reflects the activity LOG.

To make sure that KDOM is in live-state mode, it queries the Case Manager every 10s to check if a new abstraction request has been entered.

Another way to track KDOM activity is querying the CAPABLE Data Platform for Observation/Communication resources that contain KDOM component identifiers after executing an abstraction request.

When a problem with the Network/DP/CM occurs, KDOM will notify this in the log and continue trying to connect to the service.

Monitoring the Goal-based Comorbidity (GoCom) Decision-support component:

GoCom is logging multiple events of Communication with other components as well as functions that are executed by GoCom itself.

The following events are being logged:

1. Communications received from the Physician DSS and Virtual Coach
2. New Medication events
3. Guideline recommendations retrieved from the appropriate guidelines
4. The patient Goal-forest
5. Drug-Drug Interactions retrieved via the RxNav API
6. Option-sets produced for the requested recommendations
7. Errors that occurred during the run
8. Communications sent to the Physician DSS and Virtual Coach

Each log entry has a timestamp and a title to indicate what is being logged.

Additionally, GoCom polls the Case Manager every 120 seconds. The polling can be used as an indicator of the liveness of the component.

The log is saved in a file using log rotation and can be accessed with a live logs tail on the operating machine.

Monitoring the Virtual Coach:

Virtual Coach (VC) employs a standard logging mechanism using the SLF4J and Logback libraries and generates rotating log files (one file per day) with the following information:

1. events reported to VC by CM,

2. CIGs invoked by VC on the Deontics Engine for specific patients,
3. interventions generated for specific patients,
4. errors occurring during VC operations,
5. queries executed on DP and resources retrieved from DP,
6. resources generated by VC and stored in DP.

Each entry in the log indicates the timestamp and a specific actor (module) in VC that created that entry. Moreover, it includes information dependent on the type of entry, for example, in the case of CIG invocation it indicates the CIG name (corresponding to the PROforma file) and the ID of a patient for whom the CIG is executed. This allows tracking the internal operations of VC (with a special focus on errors and ways to handle them) and interactions with other components.

The log format follows widely adopted conventions, thus the generated files may be processed by more specialized tools (e.g., dedicated log viewers and analyzers). Moreover, it is controlled through a template file and can be easily changed without a need to modify VC. It is also possible to adjust the level of log details through dedicated configuration settings - specific log entries may be enabled or disabled (e.g., those related to operations on DP that are especially useful during tests and debugging, may be redundant in regular operations), and made more or less extensive (e.g., information about reported events may be enhanced with references to associated FHIR resources).

Monitoring the Sensors Module:

Sensors module uses a dedicated Node.js logging mechanism (*morgan logger*). This logger collects the HTTP requests, which are saved in an `access.log` file. Each entry in the file contains:

- ip address from which the request was sent
- date and time
- request type (POST, GET...)
- request url
- response code.

Requests stored in this file will give the possibility to monitor patients' enrollment to the sensors module. As an example, each "activity/subscribe" request indicates that a new patient with a given smartwatch ID has been enrolled and wants to share data within the sensors module.

Additionally, information concerning data of a certain patient's "subscription" to Sensors Module is stored in a local database (MongoDB). Each entry contains among others, the following "subscription" information:

- Patient Identifier
- Active (true/false) - information if a certain patient is enrolled in the Sensors Module. This gives information if patient's data are being downloaded, aggregated and saved in the Data Platform
- DeviceId - unique identifier of the smartwatch assigned to a certain patient

Thanks to this data it is possible to monitor the current number of enrolled patients, who have their smartwatches (DeviceId) properly registered.

Monitoring the Physician DSS:

Informed patient consent/assent form, ethical committee approval, training materials, and technical manual for maintenance [D7.6]

The Physician DSS (PDSS) component writes logs to file using a rotating logfile scheme. Logging is controlled via a configuration file and the detail captured in the logs can be adjusted to allow more fine-grained logging if any problem needs to be traced.

At the normal logging level, the following events are logged:

- The arrival of MedicationRequest, Observation and Communication resources to be processed by the PDSS for any patient
- Initiation and completion of interactions with KDOM (requesting updated values for abstractions)
- The running of a clinical guideline for a patient
- Outgoing communications to other components
- Periodic automatic wakeup events, when all patients in the DP are checked to see if any time-based guideline events need to be triggered
- Any errors or unexpected conditions occurring anywhere in the component
- Any shutdown and restart that may be initiated by the server Operating System (OS).

Monitoring the Deontics Engine:

The Deontics DSS Engine service runs on the same physical Virtual Machine (VM) as the PDSS and keeps timestamped logs of all engine activity, including:

- HTTP connections from components that use the Engine service (VC, GoCom, PDSS)
- Execution of guidelines on the server
- Any errors and software exceptions that occur during processing

Monitoring the patient app and the clinician dashboard:

The Patient app and the clinician dashboard logs serve the purpose of error and exception debugging, as well as monitoring of doctor and patient interaction with the system.

Currently, the following events are logged:

- Logging of api / web application errors or exceptions that occur during processing, which is stored in the default laravel.log file in the file system of the server
- Logging of specific patient-related actions conducted by a Doctor or a Patient (Activity log). Stored in the Journal table in the database
 - <date> Account created
 - <date> Patient personal information updated.
 - <date> Patient enrolment completed
 - <date> Treatment prescribed <date> Treatment taken by patients
 - <date> Goal set
 - <date> Activity set
 - <date> Symptom reported by Patient/Caregiver/Doctor
 - <date> Scheduled visit
 - <date> Visit completed
 -
- Logging the dates of last visit to certain tabs by the doctor. Information such as Doctor id, Patient id, Tab name and date are stored in the DoctorLog table in the database

Monitoring the Virtual Machines and Operating Systems (OS-VM)

For ICSM, the virtual environment is provided by Microsoft Azure (Cloud), connected to the hospital network via a Virtual Private Network (VPN) LAN to LAN, to ensure encrypted data transmission. Each partner is provided with a dedicated VM and all the VMs are able to communicate within the same network. External access is protected by firewall rules set up by the ICSM IT staff. The IT staff is responsible for checking firewall logs and identifying possible threats.

It is possible to set up automatic monitoring of critical infrastructure components, using dedicated software solutions, able to provide monitoring of all mission-critical infrastructure components including applications, services, operating systems (OS), network protocols, systems metrics, and network infrastructure.

In NKI, the health of the VM's is monitored daily. In addition, alerts have been set for (imminent) malfunctions.

The VMs are redundant, spread over 2 geographically separated data centers. There is 24/7 security monitoring on the environment (SOC).

Management of critical software updates

The basic software toolbox has been chosen by any component developer at the inception of the CAPABLE project, and approved by the CAPABLE technical management staff, and the choices have been shared among the partners to ensure the proper interaction of the components developed. In particular, every component relies on the Java VM, a REST Framework for interconnecting with others and the HAPI framework for managing HL7 FHIR Resources and related messages. Specific components also add a layer concerning their exposed service. For example, the DP relies on the OMOPonFHIR open source framework developed by GeorgiaTech University (<https://omoponfhir.org/>) and PostgreSQL as a database while the Deontics Engine relies on proprietary software developed by them. Finally, the KDOM relies on Microsoft Azure enterprise framework. For all of them at the very bottom of the toolbox stack are the OS-VM that are directly provided by the IT departments of the hospitals where the pilots are scheduled.

We believe that the toolbox components were the most adequate at the time it was put in production and no major bugs nor security issues were known. Moreover, a penetration test on the final system as a whole has been planned by an independent consultant agency of NKI.

We cannot exclude that security issues will be publicly announced concerning any of the components during the pilot, including the OS-VM. While the toolbox has been updated during the development process, it has been considered fixed by the production of the final release which has been tested.

On this basis, since the pilot time frame is rather limited (1 year), we will not consider "porting" the system to newer releases of the basic software toolbox. Of course we will be willing to incorporate security patches produced by the open source community if any emerge during the pilot trial.

As for the OS-VM that are usually the most critical component, they are provided directly by the clinical settings. The OS-VM are initially set up by the hospital IT staff according to the requirements provided by each partner. Each partner will be responsible to identify possible critical updates in the OS and take the proper actions.

Backup procedures

One important activity required to comply with the Data Protection Impact Assessment (DPIA) is to perform periodic backups of the system components. Backups are also useful in case of malfunctioning, data corruption and user errors or other unforeseen events. Backups capture and synchronize a point-in-time snapshot that is then used to return data to its previous state and the goal is to ensure rapid and reliable data retrieval should the need arise.

For ICSM, backup functionalities are provided as an additional service by Microsoft Azure. Each VM will undergo an independent backup process, with the possibility to personalize the backup schedule. Best practices suggest a full data backup should be scheduled to occur at least once a week, often during weekends or off-business hours, so a retention period of seven days is recommended.

Issues management

In this section we present a plan to manage the issues that might rise when the system will be in use during the study. The issues will be classified in the following categories:

- system-related issues: wrong behavior of the system or technical unavailability of one or more components
- device-related issues: device malfunctioning or wrong use by patients
- user-related issues: mistakes or misunderstanding by a single user (including wrong data reporting, missing data input)

The issues can be detected by:

- users
- developers during regular system maintenance
- technical/research staff

Issues reporting

According to the subject who detects an issue, different procedures are foreseen.

1. Issues detected by users: as described in Section 3, users will be trained to report any issue to the contact point at the hospital, who is responsible to trigger the support chain in order to solve it. When a user reports an issue, the contact point will ask to describe it and he will check if it is reproducible. Users are also trained to wait for further instructions without taking any personal action, until the contact point returns to them.

2. Issues detected by developers during regular system maintenance: when a developer, responsible for a specific component of the CAPABLE system, detects an issue, first identifies the component(s) affected and the impact of the issue on the functioning of the system. If other components are involved, the other developers are informed through the project management platform (Basecamp). After this initial assessment, the developers decide if there is the need to inform the contact point, who is responsible to alert the users. In any case, he must fill in a registry that keeps track of all identified issues (issue tracker registry).

3. Issues detected by technical/research staff: during testing, training or support it is possible that any issue is detected either by the contact point or other member of the technical/research staff. He must fill in the issue tracker registry and activate the support chain.

Issue management

According to the entity of the issue, three possible management options are foreseen:

1. inform a single patient/user to stop using the system until the issue is solved
2. stop a single component and inform all the users of the consequent changes in the system behavior
3. stop all the services and inform all the users that the system is down for maintenance

The contact point is responsible for any communication to the end users.

The issue management process is managed by developers using the project management platform and dedicated TF1 meetings if needed.

Once the issue is solved, developers communicate to the contact point the next actions to be performed and update the issue tracker registry.

New releases

During the pilot, we do not foresee new releases of the system with the aim of providing new functionalities, as the system will have the complete set of functionalities before starting enrolling patients.

If major issues happen, a new release might be necessary. In this case, back-end components and physician dashboard's new releases will be managed by each partner and scheduled in accordance with the technical staff of the hospital, who will be responsible to inform all the users of possible malfunctioning during maintenance. For the patient app, the patient will be contacted by the contact point to install a new version, or required updates will be managed remotely through a Mobile Device Manager (MDM) software.

Technical maintenance of the devices

The devices that are given to patients during the study are smartphones and smartwatches. All patients who accept it, will be equipped with the Asus Vivowatch 5 smartwatch, to be returned at the end of the study. Regarding the smartphones, patients who own an Android smartphone compatible with the CAPABLE app requirements, can choose if they want to use their personal phones or to use the one provided by the project. The project will provide a smartphone to all the other patients, to be returned at the end of the pilot study.

All the devices are managed by the hospital responsible for the clinical study. The technical staff of the hospital takes care of the maintenance of the devices. The technical maintenance includes:

- ordinary maintenance: software updates, account management, data traffic plan renewal, basic protective measure against accidental damages, procedures related to the end of study.
- extra-ordinary maintenance: management of damages and malfunctioning

The physical maintenance of the devices is left to the patients as the main users who are preliminarily trained on the basic actions to guarantee a correct and continuous use of the devices. The ordinary maintenance of the software installed on smartphones and smartwatch is performed through a MDM system.

The MDM system allows administration of several devices at the same time through a dashboard accessible to the technical staff of the hospital. Through the MDM it is possible to prevent the usage of undesired apps, to force updates on selected apps, to shut down

Informed patient consent/assent form, ethical committee approval, training materials, and technical manual for maintenance [D7.6]

the smartphone, to wipe up the data in case of unauthorized access, to provide remote support, to broadcast messages, to prevent the process of biometric data as not included in the allowed data processing.

Any physical damages of the project devices should be promptly reported by the patients to the contact point at the hospital. Patients are informed not to take any personal initiative trying to solve these situations. The policy for physical damages foresees the replacement of the device with a working one. Malfunctioning of the devices (for example: failure to couple smartwatch with the smartphone using Bluetooth) should be also reported to the contact point. In this case, the policy is that the contact point will provide support to the patient to solve the issue and if it is not possible, to replace the device.

5. Conclusions

In this deliverable we have presented the activities of WP7 related to the preparation of the CAPABLE pilot study. These activities involved the participation of all the project partners, in a multidisciplinary effort including clinical, technical, and legal experts. The main challenge was related to understanding the regulatory setting and to decline it into the specific national requirements and into the local organizational framework of the hospitals. Once the workflow of the activities to be carried out was clarified, a consistent effort was needed to prepare the high number of required documents, complying with the timing needed to complete all the authorization procedures.

The main outcome of these activities is that all the documentation has been submitted to the relevant authorities on time and we foresee that the pending approvals will be cleared by the end of Month 37.

6. Annexes

Section 2

Checklist security measurements template:

EN: [Check-list_securitymeasure_ENG.pdf](#)

Data Protection Impact Assessment (DPIA)

ITA: [CAPABLE DPIA sottoscritta.pdf](#)

NL: [CAPABLE DPIA NKI v3 31052022.docx.pdf](#)

Study protocols

ICSM: [CAPABLE Clinical_evaluation_plan.pdf](#)

BARI: [Protocol Bari.pdf](#)

NL: [C1. Study protocol CAPABLE NL81970.000.22 v2 17112022.pdf](#)

Informed consents

ITA: [Locati Capable ConsensoPazienti.pdf](#)

[CAPABLE Bari ConsensoInformato.pdf](#)(English translation:

[Locati Capable InformedConsent_ENG.docx](#))

NL: [E1-E2. Informatiebrief en toestemmingsformulier proefpersonen CAPABLE v2 17112022.pdf](#)

(English translation: [Informed consent CAPABLE NKI English.pdf](#))

Privacy statements

ITA: [Locati Capable Informativa.pdf](#), [Informativa privacy BARI.pdf](#)

NL: [E1-E2. Informatiebrief en toestemmingsformulier proefpersonen CAPABLE v2 17112022.pdf](#)

Final Ethical Committee approvals

ICSM: [CAPABLE CE 2741.pdf](#)

BARI: [Approval Bari.pdf](#)

NKI: [METC Approval P1a. Besluit positief MDR art 62.1 NL81970.000.22 versie 01 d.d. 28-12-2022.pdf](#)

Medical Device Authorization documentation

ITA:

first

version: https://drive.google.com/drive/folders/15bgGE8jiF6ahYb0WdQYO7WK3p8hfYoIB?usp=share_link

revised

version:

<https://drive.google.com/drive/folders/1HfaweP0gojKy5uj7aZSxpfqvrKGxJ4OW?usp=sharing>

Validation letter: [2099_convalida della domanda.pdf.pdf](#)

NL: https://drive.google.com/drive/folders/1nh6E34RMsm-cR6-NDqpuNm07tqD8OU12?usp=share_link

Validation letter: [CCMO Approval P7. Positieve validering MDR-klinisch onderzoek NL81970.000.22.pdf](#)

Section 3

User manual clinician dashboard

ENG: [istruzioni del fabbricante dashboard.pdf](#)

ITA: [CAPABLE Istruzioni dashboard ITA v1 1.pdf](#)

User manual patient app

ITA: [CAPABLE Istruzioni app ITA v1 1.pdf](#)

NL: [D3. CAPABLE Instructions for Use Patients Dutch v1 17112022.pdf](#)

EN translation: [istruzioni del fabbricante mobile app ENG.pdf](#)

Video tutorials (example for symptoms reporting):

ITA subtitles:

https://drive.google.com/file/d/1G9dIFr8U6vzmPvkXdsN4u9I9a68vQ1bi/view?usp=share_link

EN subtitles:

https://drive.google.com/file/d/1JEp1Fj8YxnRMIHKxoVN_3jTd5FIoTeuU/view?usp=share_link