CRANE

Scope document

Dissemination Level:	**PU**
Deliverable Type:	**RE**
Date:	**04-05-2022**
Distribution:	**WP3**
Editors:	**Roberto Gimenez, Mónica Bouzo**
Contributors:	**ALL**

*** Dissemination Level:** *PU=Public; CO=Confidential, only for members of the Consortium (including the Commission services); EU-RES= Classified information: RESTRAINT UE (Commission Decision 2005/444/EC); EU-CON= Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC); EU-SEC=Classified Information: SECRET UE (Commission Decision 2005/444/EC)*

**** Deliverable Type:** *R=Document, report; DEM=Demonstrator, pilot, prototype; DEC=Websites, patent fillings, videos, etc; ETHICS=Ethics requirement; ORDP=Open Research Data Pilot; DATA=data sets, microdata, etc.; OTHER*

Document Summary

This document aims to define CRANE scope pointing out the needs that must be addressed during the project, the steps to do it and the main stakeholders of the process.

Funded by the European Union

This project has received funding from the European Union´s Horizon 2020 research and innovation programme under grant agreement No 965277

DISCLAIMER

The work associated with this document has been carried out in accordance with the highest technical standards and CRANE partners have endeavored to achieve the appropriate degree of accuracy and reliability. However, since the partners have no control over the use to which the information contained within the document is to be put by any other party, any other such party shall be deemed to have satisfied itself as to the suitability and reliability of the information in relation to any particular use, purpose or application.

Under no circumstances will any of the partners, their servants, employees or agents accept any liability whatsoever arising out of any error or inaccuracy contained in this document (or any further consolidation, summary, publication or dissemination of the information) and/or the connected work. CRANE disclaim all liability for infringement of third-party rights and any loss, damage, expenses or claims suffered by any person using the information.

The contents of this document are the sole responsibility of the CRANE consortium and can in no way be taken to reflect the views of the European Commission.

Table of Contents

List of Authors

Partner	Authors
EUROB	Roberto Giménez, Mónica Bouzo

Document History

Date	Version	Editors	Status
22-March-2022	0.1	Mónica Bouzo	Draft
31-March-2022	0.2	Roberto Giménez, Mónica Bouzo	Draft
6-April-2022	0.3	Roberto Giménez, Mónica Bouzo	Draft for review
11-April-2022	1.0	Roberto Giménez, Mónica Bouzo	Final version
25-April-2022	2.0	Roberto Giménez, Mónica Bouzo	Section 4. Information reorganization for clarity
04-May-2022	3.0	Roberto Giménez, Mónica Bouzo, Ingrid Kjorstad, Robert Hogvall	Section 3 minor updates

List of Figures

List of Tables

Glossary

Acronym	Meaning
AI	Artificial Intelligence
CoED	Computing on Encrypted Data
DPIA	Data Privacy Impact Assessment
EU	European Union
GDPR	General Data Protection Regulation
HTA	health assessment
ICT	Information and communication technologies
KPI(s)	key performance indicator(s)
MPC	Multiparty Computation
NGO(s)	non-profit organization (s)
PCP	pre-commercial procurement
R&D	Research and development
SMC	Secure Multiparty Computation

Introduction

CRANE is a European H2020 pre-commercial procurement (PCP) project. PCP is an approach where the public sector challenges industry to develop innovative solutions tailored to its need. In this case, CRANE will address the comprehensive treatment of chronic diseases in rural areas looking for an integrated self-care model to improve chronic patients' wellbeing.

CRANE consortium gathers together the knowledge of seven partners from four European countries. The group includes members with complementary knowhow in PCP execution, co-design method, experts in health data management, ICT architecture, health economics and integrated care as well as in management and development of European projects. CRANE also involves three rural regions from 3 different European countries which are new procurers in the EU PCP field. The lead procurer is Region Västerbotten (Sweden), and the buyer's group is completed with Extremadura (Spain), and Agder (Norway). Despite their cultural differences, these regions share a common and urgent need for health and care innovation caused by their growing elderly population.

To succeed is necessary to wisely design a model able to meet patients' and caregiver's requirements and carefully plan the steps to develop it. For that is crucial to get insights into the needs of the target groups and to engage in the project as many stakeholders as possible. CRANE member organized several workshops with different groups of stakeholders in the three procurer's regions. After those events, the consortium members met in person in Jarandilla de la Vega (Extremadura) for four days to analyse all the inputs received and set the OMC roadmap. Among the requirements for the OMC arise the need to prepare this document to define CRANE scope presenting the problem to address, the goals of the project and the plan to achieve them. The scope document is a key document that provides all stakeholders with a **clear understanding of why the project was started and its purpose.**

1. CRANE Overview

Europe is facing a demographic challenge posed by an ageing population that demands more healthcare from an already stressed system. The exponential growth of the elderly population will make that 30% of the Europeans will be over 65 years in 2050 compared to the 20% in 2020. **Ageing is more prominent in remote and rural regions where only 20% of chronic patients can be guaranteed full attention by social service and primary care entities.** Thus, the urgency to move 70-80% of patients to self-care and self-monitoring impulse the need for self-care innovations. Additionally, more than 30% of Europeans over 65 lives alone requiring technology user-friendly for them.

Municipalities are vulnerable to healthcare overload when more than 19,5 % of the population is over 65 years and cities in developed countries are expected to pass this level in 20 years or less. To anticipate this situation CRANE will address the comprehensive treatment of chronic patients in three rural areas with more than 30% of the population over 65- an average age not currently found in urban areas. Region Västerbotten in Sweden, Extremadura in Spain, and Agder in Norway will serve as testing grounds to build sustainable healthcare and social care solutions transferable and scalable to a larger city context.

CRANE envisioned an evolution toward a model where more than 80% of chronic patients move to self-care, supported by two pillars: healthcare from home and the system for health and wellbeing. Healthcare from home and self-monitoring bring to the home interactive technology, supported by intelligent use of data, to provide smart personalized treatment. The system for health and wellbeing

is an extended concept of integrated care, to empower citizens and offer them essential elements of well-being tailored to each individual's needs. It includes the health and care services, family, services providers, etc.

This integrated care approach aims to provide a flexible, dynamic and personalized self-care system. The tools to build up such models are a data lake and an open platform. CRANE point of departure is that each citizen is the owner of their own health data and that those data together with public data should become actionable support for those at risk or with a chronic condition. CRANE model will help change citizens' self-conception from being passive patients to become active citizens again managing their health conditions. CRANE makes public data and personal health data obtained through consent, automatically accessible. Then, applying intelligent technologies provides new smart and tailored insights. Unlike current siloed health and social care provision, CRANE provides the citizen with open and trustworthy control of their own data and its use.

Figure 1. CRANE model pillars

In the end, CRANE looks for a technology-enabled all-in-one service, adaptable to different European healthcare systems and flexible to tailor the CRANE model to each of the participant procurers complementing existing public resources with a public-private partnership. This requires engaging all critical actors necessary to disrupt the current service models: citizens, eHealth and welfare tech industry as well as healthcare and social service providers (private and public). A single vendor is insufficient to design and develop such a complex public-private network to share and use data, making PCP the most suitable instrument to do it with several service providers.

2. Stakeholders

In a project, the stakeholders are those individuals or entities with an interest or concern in its activities and outcomes because they are positively or negatively affected.

The consortium has identified several stakeholders to engage in the course of actions undertaken by CRANE that can be classified into three main groups:

1. **Direct PCP participants:** This group includes any potential R&D provider that could participate in the project, typically Digital Health and IT companies.
2. **Relevant actors:** Includes any entity or individual affected by CRANE outcomes like buyers, health and care professionals, demanders (patients and any potential final consumer), policymakers, any authority interested in CRANE solutions and future procurement including public authorities or patients' and carer's organizations.

3. **General public.** Includes any person for which CRANE initiatives and results are meaningful such as media sources, university students and society in broader terms.

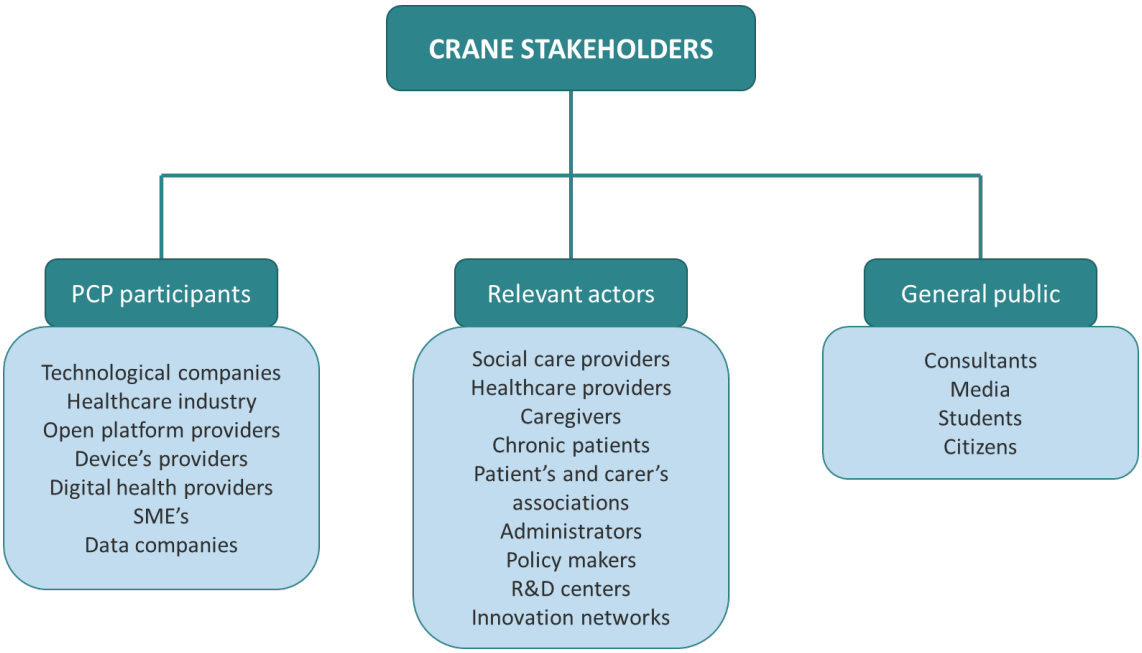


Figure 2. CRANE stakeholders' examples

3. CRANE SCOPE

3.1. Building blocks

CRANE consortium envisioned the development of the project in five building blocks

Data governance

The first step toward CRANE model is to make citizens aware of the importance to become the owners of their health data. Health data belong to individuals who have a right of control over their own data (fundamental right to data protection) within the limits and under the conditions defined by the Charter of Fundamental Rights of the European Union and national laws. However, they can not only improve citizens' health and well-being but also be used for the greater good and the achievement of the public interest, when shared appropriately.

CRANE model aims to gather public data and specific data from patients for their own benefit through a private and secure consent platform that not only complies with General Data Protection Regulation (GDPR) but also enhance the use of personal data. The starting point for that will be to create the data repository and establish a governance model that ensures its privacy and security. The dialogue with experts in the field, allows us to define a **theoretically viable governance model for the project repository**. A governance model implies that in the case of any request, decision-making processes will be standardized and based on the evaluation of the request's requirements. This obviously does not exclude the rejection of requests when:

- The defined requirements are not met.
- There are no resources available to deal with them.

Two types of uses of data shall be distinguished irrespective of their nature:

- Primary uses: those directly related to the provision of care in healthcare services.
- Secondary uses:
    - The use of the data for historical, statistical or research purposes, when these purposes are not considered primary by the applicable legislation, the entrepreneurship and any other legitimate purposes by the legislation on transparency and/or re-use.
    - Processing involves data analysis for the definition of public policies, for the improvement of the quality of service and organisation, and for any other purposes that directly affect the decision-making processes of the entity for non-directly care purposes.

Proper governance of the Repository should provide for the existence of:

- *Corporate governance body*: supervisory body to which substantial decisions can be attributed in terms of defining the policies of the Repository and controlling its functioning in the main areas (economics, general terms and conditions, activity reports, partners admission…)
- *Assignment Committee*: The body assigned the task of final approval of the processing of data in any form.
- *Ethics committee*: in this case the Repository may take into account different alternative or complementary operational criteria:
    - to include a catalogue of committees, e.g. hospital and/or university committees, whose ethical functions are to be verified and formally recognised;
    - to have its own body to which ethical verification functions are assigned;
    - to agree with an external existing committee for the evaluation of applications.
- *External advisory committee*. A plural body formed by experts among the stakeholders of the project. It could integrate and define, within the framework of the committee, some small, permanent, full-time units that would contribute to the Repository's monitoring.
- *Management bodies*: bodies and/or functions necessary under the legislation in force or with the Repository's own needs for its ordinary functioning like data protection staff, data analyst or security officers and/or security committee.

From the point of view of regulatory compliance conditions and management needs, it is necessary to define different procedures depending on the scenario of the use of the Repository. These procedures may be autonomous or interdependent. For this purpose, the following procedures are identified as possible:

- *Membership procedure*: Procedure for new partners to join the Repository.
- *Registration procedure*: Procedure ordered to the registration in the system of its users. This aims to ensure that users are aware of and accept the terms and conditions of use of the platform, awareness of additional obligations that may derive from sectoral legislation and the security traceability of the information.
- *Access procedures with specific legal requirements*: Procedure for the declaration of processing operations subject to data protection regulations (exercise of the GDPR rights, complaints and claims or requests for access to and/or use of data requiring an ethical impact assessment related to Artificial Intelligence (AI)).
- *Monitoring procedures*: audits and controls regarding ethics, information security, data protection, quality, costs etc.

Trend technologies

The next step will be to ensure that cutting-edge innovation and trend technologies are applied to the system to make the most of the collected data. A **data lake** can in a simple form serve as a safe harbour to store personal health data for citizens. But CRANE aims to develop a more advanced data lake designed to enable a sophisticated patient centered and wellness promotive portfolio of services as well as to different research, innovation, and development activities. It is essential to provide an integrated system approach where data can flow free ensuring interoperability and long-term durability. For that it will take into consideration legal and organizational challenges, especially considering the need for sharing of information across different arenas and healthcare providers.

CRANE model will be able to utilize data generated from both citizens/patients' own IoT devices as well as from IT systems within public and private organizations with an overarching service solution based on dynamic ecosystems and AI. The adequate monitoring and intervention technology along with intelligent use of data could drastically reduce the need for professional healthcare and reduce the workload for healthcare services. This is especially important in remote and rural areas where the available economical and human resources are limited.

To ensure its success is also needed to build trust with the patients through **transparent and open policies** as well as applying a feedback system to demonstrate benefits for the individuals, both in the short and long run. In this context, CRANE will base its platform on the latest encryption technology to develop a secure public-private data lake platform.

The CRANE MODEL will be able to:

- Give access to and analyze monitored signals, in combination with the EHRs (electronic health records) and other available data, to generate useful information, and generate alarms or warnings to both caregivers and the patient.
- Make use of all collected data to dynamically update identified needs, priorities and activities of all stakeholders involved.
- Use the CRANE data for both specific solutions and to create and develop new insights.

To implement this CRANE model, it will be necessary to consider compliance to important privacy regulations:

- GDPR: data protection certification mechanisms and/or codes of conduct.
- Standard certified mechanisms: on privacy, security, de-identification and/or anonymisation and pseudonymisation, AI and Secure Multiparty Computation.
- Data Privacy Impact Assessment: could be necessary before authorization to the privacy data treatment and should follow the guides of the Authorities on Data Protection DPAs from the three CRANE countries (Norwegian Data Protection Authority Datatilsynet, Spanish Data Protection Agency AEPD, Swedish Data Protection Authority) plus the European Data Protection Board EDPB.

In Norway, it is also a privacy requirement that a citizen should be able to control what information that should be available for health personnel.

Garden for care

The multidimensional needs of the individual would require more than just technology at home. The garden of care around the patient, which starts with healthcare and social care services, needs to be

flexible to adapt dynamically to each person's needs and the social context. CRANE garden of care will implement an appropriate well-being ecosystem into the solution helping to:

- **Make health care from home a reality**: CRANE will address the current data management challenges, with professional insecurity and concerns regarding data and issues from home monitoring and self-care. CRANE will apply intelligent use of data and design a sophisticated data management system.
- **Ensure that health data belongs to the citizen**: From a legislative perspective, a healthcare or social care provider is required to record selected parts of the health data generated in healthcare visits, in the electronic health records. In CRANE, healthcare personnel will register health data, and validate the quality of the data. But the health data still belongs to the citizens who through GDPR and EU Data governance act are entitled to access to and shall be able to control the use of any data produced that concerns the citizen.
- **Make health data available for the citizens**: Any health data generated through an individual shall be made available for the citizens through MyHealthEnabler, similar to a subscription of information from different health data sources. MyHealthEnabler will display CRANE users' health data and the data they want to see while serving as a place where users provide consent for any other body to view the data.
- **Favour insights and empowerment (potentially based on AI and Machine Learning)**: Users of MyHealthEnabler will through their health data set be able to generate insight regarding their current health condition. Insights for users of MyHealthEnabler will be developed by comparing MyHealthEnabler users' data with data in a health data lake. Insights will inform users of MyHealthEnabler about their current health situation, what looks to be on track as well as what looks to have a direct negative development/impact on CRANE users' health and well-being. Insights on negative development can be different such as:
  - insights that require immediate attention
  - insights aimed at avoiding future negative health and well-being consequences
  - Insights that confirm that CRANE users' health is OK.
- **Matching insights with actions**: CRANE will match the MyHealthEnabler users' current health situation with appropriate actions to be taken. The service offers can be identified among public healthcare and social care providers as well as from the wider local community. The appropriate set of services proposed through CRANE, by CRANE collaboration partners aims to improve citizens' health and well-being. Services available need to be pre-assessed to fit CRANE platform.
- **Gather local services**: CRANE will be a platform to which local service providers and companies can be connected. Garden for Care is an enlarged healthcare community, that beyond healthcare and social care services also includes tailored offers from NGOs, private service providers, other companies such as innovation industry actors as well as wider municipal services. All services offers provided through CRANE platform are based on a match with the current health condition, and the latest health data generated but also on health trends among CRANE users. Service offers should motivate the citizens to comply and adhere to improve their health conditions and continue with the self-monitoring and self-care so improved health and well-being are achieved. This will also secure continued insight into the progression of the citizens' chronic condition(s) and help citizens to stay autonomous for a longer period.

- **Offer more than automation**: CRANE solution cannot only be a stand-alone automated solution, clear and simple ways to contact healthcare and social care services need to be built and alternative routes for CRANE users to seek information from. CRANE shall be able to compile an appropriate set of data and information so users, can make this available for the healthcare and social care services. An appropriate overview of the patient's health status will help professionals to become more efficient and effective and reduce possible data overload.

People matter

This CRANE building block aims to empower patients to get in control of their health through motivation and self-esteem improvement. Empowering citizens and improving their well-being will help people to find other ways to stay healthy reducing the use of traditional healthcare and social services. In this way, the workload in health and social care will be lower allowing these providers to improve their quality of work.

People matter relates to the understanding of the citizens with chronic conditions for CRANE service package during a pilot and validation phase. It is necessary to help people increase their autonomy in the health data ecosystem and ensure their ability to use the services through education and the appropriate tools to enhance their digital and health literacy. Increasing engagement with the system is decisive to develop intuitive solutions and ensure training for patients and professionals. The system needs to proactively engage with the users and suggest appropriate actions at the right time, which triggers the users to take the right action to promote their well-being. An accurate individual's profile can help to match citizens with the services they need. So, getting to know the CRANE users will secure that CRANE services will contribute to improved health and well-being. Some of the most important aspects to consider when designing how to get to CRANE users are outlined below:

1. **Secure compliance and adherence to CRANE model**
   Individually designed through personal motivational schemes. Motivation will be identified through tests and assessments of MyHealthEnabler users, be identified. Individual profiling of CRANE users will serve as an important input when generating automated service proposals to improve health conditions and well-being. This is connected to a range of factors that can be monitored such as health data but also other biodata. The system needs to be dynamic, responding to changed conditions in the CRANE user's perception of what is healthy for them. Equally important are the psychological aspects of users, such as understanding their motivation and behaviour so CRANE users recognize their individual profile in CRANE.
2. **Ensure trust and safety**:
   Citizens often meet a new professional when they have a healthcare appointment due to a shortage of qualified healthcare and social care professionals, especially in remote and rural areas. This makes them describe their situation over and over again creating frustration and mistrust of the current system. CRANE system can generate tailored descriptions for the citizen to share helping restore trust and improve the perceived level of safety in healthcare and social care services. To secure trust and safety CRANE must consider:
   Digital literacy: Offering training of the services to professionals and CRANE users is crucial for the system to succeed. Studies of transformed service models in Nordic regions show a range of examples of how training can be conducted, such as the Norwegian training package "Velferdsteknologiens ABC" (The ABC of Telecare) for social service providers. The Finnish region EKSOTE has a training program for their newly recruited staff which includes work at

their ICT unit to create an understanding of the power of health data and the need for data-driven healthcare and social care.

Health literacy. Citizens' exposure to health data will increase when CRANE makes health data from different sources visible (siloed data from healthcare and social care entities, data from sensors and monitoring devices…). This increased exposure will to a different degree create a level of uncertainty among the citizens requiring to explain what their health data means. CRANE must provide information in a format to citizens, so it reduces any uncertainty related to their chronic condition. A proposed solution to consider is to connect to healthcare providers' official channels to improve the citizens' health literacy, to secure that a user of CRANE can get adequate information that builds and secure trust in CRANE services.

3. **Segmentation of patients:** CRANE model shall/should improve people's ability to self-manage their health and well-being. This means that CRANE need to know their users and through segmentation of users find the best match of services for the individuals. To segment patients, we can consider:
    - Biodata such as age, where do users live, how do the users live, current or previous work experience etc.
    - Health data input from self-monitoring, to provide insights for the users and target appropriate and necessary actions.
    - Motivation and behavior to ensure that proposed response to improve health are motivating the citizens to take action. A system shall be designed to be adaptable to the ability of the citizens (health and data literacy), as well as more current energy level citizens experience based on data on how the citizen has slept, resent exercise, stress level etc.
    - Use of current state of mind assessment: Simple frequent feedback, for instance, use of smileys such as red, yellow and green to indicate the current level of motivation
    - The user's context: Who are their loved ones, the user's local community and how do they wish to involve the loved ones and their local community.

Value-based model

There is a lack of adoption and dissemination of the health innovations needed to drive the implementation of important breakthroughs in value-based healthcare, and therefore important breakthroughs in knowledge often fail to be translated into medical practice. The last building block in CRANE is centred on providing a **value-based model and key performance indicators (KPIs) to assess the efficiency and the potential value of innovations that are still under development** to create value-based procurement recommendations.

CRANE value-based model will revolve around the patient's needs to meet the main aim of the project which is to improve patients' wellbeing. For that, CRANE will apply an **early health assessment (HTA) framework** based on the early engagement of stakeholders, systematic literature reviews and scenario analysis to estimate the potential value of the service or technology which is under development. The framework is characterized by evaluating potential stakeholder values in four domains (patient, economic, clinical and organisational) at defined stages of the procurement process with the purpose of:

- Identify unmet user needs, elements adding value to the system and those to be modified.
- Generate evidence on results
- Be ready for a value-based service procurement when the project ends.
- Evaluate the performance of suppliers and solutions in CRANE.

- Identify areas of opportunities
- Help the innovators to complete a product that the health service wants

A co-assessment tool, the Health Value Spider, is developed as part of the tools in early HTA methodology. Each stakeholder assessed the unmet user needs and potential health values of each domain.

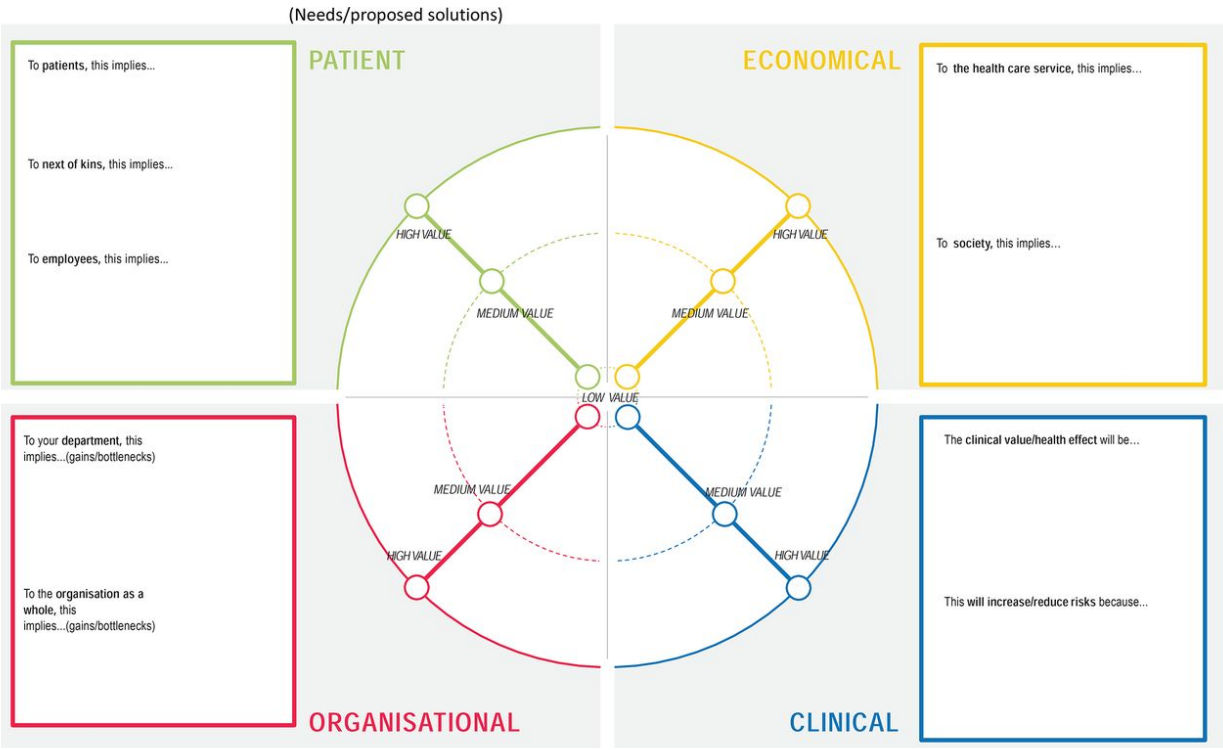


Figure 3. Health Value Spider

4. Requirements

4.1. Basic Considerations on Data Handling Requirements in CRANE

As a first exercise in CRANE, the following two points should be considered when defining your data handling framework for CRANE

Prior analysis and categorisation of the conditions for processing operations

This would involve establishing a functional relationship capable of defining when a given processing operation is lawful and proportionate following the current regulatory framework. This is a dynamic requirement and one that is intended to grow with the platform. It should also be noted that it is a step in the design of the management process. However, it is also proposed as a prior standardisation effort that contributes to having an available catalogue of services defined by the Repository procedures. In this regard, at least the following parameters should be considered for each usage scenario:

1. Applicant of the processing.

- Research Body
- Public Healthcare Sector
- Private Healthcare Sector
- Private individual or legal entity

- Individuals or entities from third countries (non-European Union or non-European Economic Area countries)

2. Purpose and type of use.

It is ordered to facilitate the judgement of the lawfulness of the processing and its proportionality as well as its assessment from the point of view of ethics.

3. Categories and volume of data.

Concerning the previous criterion, it allows applying the principle of data minimisation and assessing the potential impact on the rights of the data subjects if personal data are involved.

4. Applicable legal framework. Consistency or purpose relationship.

It allows, given the purpose requested, to define both whether the request should be complied with and the specific qualitative, quantitative or temporal conditions under which it may be complied with or the reasons for a possible refusal.

It also makes it possible to distinguish between cases of open access not requiring prior authorisation and cases requiring an authorisation procedure.

5. Frequency/standardisation.

It allows defining those cases that can be standardised either from the point of view of data access (data operations) or from the point of view of data processing. The expected result of this requirement is to be able to define processes that can be automated from the management's point of view. It implies a prior analysis and classification effort. However, this is a sustained effort that should consider the evolution of the system itself in the light of lessons learned and possible incidents that may occur.

CRANE compliance framework

1. Data protection.

Develop and implement a platform General Terms and Conditions (Data Sharing Agreements). These terms, without prejudice to its general scope, should pay particular attention to:

- The conditions determining the inclusion of data in the Repository.
- The conditions for the use of and access to the data or results.
- The processing of special categories of data and data of vulnerable persons.
- The conditions for the processing of anonymised personal data.
- The implementation of a certified security standard.
- The definition of organisational roles and functions in the processes supporting compliance and decision-making.
- The possibility of implementing a sanctioning regime for cases of non-compliance with the Code of Conduct or General term Conditions

2. Reuse.

Re-use of data through the platform should:

- Define the nature, structure and conditions of the datasets
- Define conditions for the re-use of data in the following aspects:
  - General terms and conditions of the platform, infringements and penalties included.
  - Definition of the re-use request procedure.
  - Obligations of sharing and integration in the platform of research data generated in activities financed with public funds.

- Specific conditions for the use and access to the data: free access / fees, standard licences and open licences, exclusive agreements, and access requests for re-use.

4.2. CRANE Overall Approach to Legal and Ethics on Data

The tenders must address the principles and values of the Project by ensuring a high level of privacy and information security through a design focused on guaranteeing users' rights. In addition, the ecosystem of "CRANE Applications" must apply the inspiring principles of biomedical ethics and the new requirements defined by the European Union in the field of artificial intelligence. To this end, it will be essential to:

- Ensure the fulfilling of the data protection principles of the GDPR.
- Propose robust consent models that offer maximum control and traceability to patients.
- Focus on accessible and understandable design that strengthens patient empowerment.
- Apply the methodologies of data protection by design and by default at all stages of development and throughout the lifecycle of the processing.
- Develop a data protection impact assessments and AI risk assessments based on the Assessment List for Trustworthy Artificial Intelligence (ALTAI).
- Propose technology that provides proper security, resilience and interoperability of information systems.
- Develop anonymisation processes by the conditions and methodologies defined by the European Data Protection Board and Data Protection Authorities.

The design of any processing, application or IT system for CRANE must follow the methodologies and processes defined by the General Data Protection Regulation. These methodologies are based on the so-called "data protection by design and by default" and incorporate the following legal, technical and ethics requirements:

1. Compliance with the GDPR

While data protection regulation such as the GDPR makes some existing uses of sensitive data illegal, the larger potential gains from utilizing data remain. The solution is to not stop using sensitive data, but to find a third way that allows its positive use.

Several mature and promising cryptographic techniques exist, which provide strong protection of data at various lifecycle stages. However, the chain is no stronger than the weakest link, and integrating these technologies efficiently and securely is often a hard challenge. Solutions must offer strong protection by integrating state-of-the-art cryptographic techniques for the protection of sensitive data during the full life cycle of use (at rest, in transport and during the process). One class of solutions makes data itself anonymous, although this degrades the value of the data. Another class allows analysis of the sensitive data in detail by the use of “computation on encrypted data”, with SMC as one of the most efficient approaches.

2. Risk-centric approach

The design of any data processing must consider the risks to rights and security. The GDPR requires the use of a specific methodology, the data protection impact assessment (DPIA) when processing special categories of data on a large scale. The DPIA positive lists of Data Protection Authorities (DPAs) additionally impose this obligation when data of vulnerable persons, minors, or innovative technologies are processed.

CRANE Tenderers should consider the following DPAs' guidelines and criteria in this issue.

Guideline	Authority
Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)	European Data Protection Board
Norway SAs list of the kind of processing operations which are subject to the requirement for a Data Protection Impact	Norwegian Data Protection Authority (Datatilsynet)
Sjekkliste for vurdering av personvernkonsekvenser (DPIA)	
List of the types of data processing that require a data protection impact assessment under art 35.4	Spanish Data Protection Agency
Gestión del riesgo y evaluación de impacto en tratamientos de datos personales	
List regarding Data Protection Impact Assessments according to article 35.4 of the Data Protection Regulation	Swedish Data Protection Authority
Varför ska man göra en konsekvens-bedömning?	

Table 1. Risk-centric approach regulatory guidelines

3. Data Protection by design and by default

The application developments proposed by the tenderers shall ensure the methodologies of data protection by design and by default as required by the general data protection regulation. These processes shall be documented and evidence of compliance shall be generated. Particular consideration shall be given not only to the general recommendations for GDPR compliance but also to any specific recommendations depending on the technology developed.

CRANE Tenderers should consider the following DPAs' guidelines and criteria in this issue.

Guideline	Authority
Guidelines 4/2019 on Article 25 Data Protection by Design and by Default	European Data Protection Board
Privacy by design (Recommendations on shaping technology according to GDPR provisions)	ENISA
Privacy Enhancing Technologies (PETs)	
Software development with Data Protection by Design and by Default	Norwegian Data Protection Authority (Datatilsynet)
Artificial intelligence and privacy	
Guía de Privacidad desde el diseño	Spanish Data Protection Agency
Adecuación al RGPD de tratamientos que incorporan una Inteligencia Artificial	

Table 2.Data protection regulatory guidelines

CRANE should have a particular focus on ensuring that local data breaches have a minimal and non-escalating impact on privacy. In particular, when data is at rest, the data in a single database or on any single machine should not be identified. To this end, the provided solution could employ both pseudonymisation and encryption. To mitigate the probability of breaches during the processing of

data, the framework should allow for various solutions such as: a) moving data within a secure perimeter for plaintext analysis by approved personnel, b) using pseudonymisation and encryption during processing and c) using of Multiparty Computation (MPC) as a Computing on Encrypted Data (CoED) technology. Solutions b) and c) make the CRANE framework more broadly applicable across private and public organisations as no PII are exposed in plaintext to any individual persons. In practice, the CRANE framework should allow for a combination of technologies that best meet the concrete application.

Proposal for CRANE infrastructure data governance should also consider the seamless data protection through its life-cycle. In this way, data governance will be also in relation to CRANE Data Management Plan.

4. Control and transparency

CRANE must integrate components to allow data subjects and data holders to retain control of the data and transparency of its use.

To ensure the application of the developed framework in industrial settings, it must be developed in tight collaboration with the application of the framework in two use cases. The user consent platform will be requested to be privacy- or security-by-design that not only complies with GDPR but also should enhance the use of personal data. This is achieved by a platform that both facilitates decentralized control of personal data and orchestrates privacy-preserving use of personal data. The platform should be designed as a two-sided platform serving the two primary user groups: Citizens (controlling the use of data) and Analysts/vendors (requesting data).

The CRANE Platform will ensure that **any use of data is based on consent** and that follows the "privacy measures" specified and enforced by the consent. The privacy protection should nevertheless provide a precise description of the result or output that will be shared with the Analyst, which could be pseudonymised or anonymised data or statistical results. Secure Multiparty Computation (SMC) is the secure infrastructure that we propose to use to combine data and produce the output i.e. to meet the privacy measure. The infrastructure is required to be governed by the trusted 3rd party and the Computing Parties that run the SMC.

5. Security and interoperability by design and by default.

Security and interoperability are two essential requirements for the proper functioning of CRANE. The proposed solutions must be able to meet the highest standards of safety and interoperability. For example, for the Spanish pilot the repository manages data from the Spanish Public Health Service, then the developers must ensure that the applicable security guarantees are met in accordance with the first additional provision on security measures in the public sector of Organic Law 3/2018, of 5 December, on Personal Data Protection and guarantee of digital rights. And under Royal Decree 3/2010, of 8 January, which regulates the National Security Scheme, and Royal Decree 4/2010, of 8 January, which regulates the National Interoperability Scheme and its Technical Regulations for the development of Royal Decrees 3 and 4 of 2010.

Guideline	Authority
Handbook on Security of Personal Data Processing	ENISA
Distributed Ledger Technology & Cybersecurity - Improving information security in the financial sector	
National Security Framework (ENS)	Legal Spanish requirements
The National Interoperability Framework of Spain	

Table 3. Security and interoperability regulatory guidelines

Digital health Apps and digital therapeutics are a field with the potential to grow exponentially, especially since it has emerged a clearer regulatory framework, in both the EU and the US, around certifying digital interventions via apps (ISO 13485 & Medical Device Regulation (EU MDR)).

The CRANE solutions should focus on bridging the gap in achieving organisational interoperability, in this sense the list of technological principles of the CRANE form has been inspired by best practices.

The CRANE Open Platform should follow this **interoperability layer cake**:

- Platform: must be very prescriptive at the Technical and Syntactic levels as these standards are the most mature and most adopted by healthcare delivery and other industries.
- Semantic layer: more flexible. Language sets, clinical domain specialty modelling, and vocabulary can be used. But the focus has to be on being able to map data to other code sets for expanded use. Data in the integrated care plan should be able to be reformatted and transmitted in a usable format for the end-user.

  For example, In Norway (and many other countries), FHIR is considered as the preferred standard for information exchange on semantic level. The Norwegian directorate of eHealth also recommends using the International Patient Summary (IPS – EN 17269) as a common framework for structure and exchange of patient data. This standard has core set of information elements relevant all kinds of healthcare services.
- Upper layer (Organisational layer): This layer has to allow providers to develop new methods of care delivery, by using the platform: they will know their services, will be able to capture information and outcomes in a consistent manner that will be able to be securely, efficiently and, effectively obtain, format, and communicate.

6. Certification mechanisms and/or codes of conduct.

The GDPR encourages controllers or processors to adhere to data protection certification mechanisms and/or codes of conduct. Tenderers should consider standard certified mechanisms on privacy, security, de-identification, artificial intelligence and Multiparty-Computation

7. Auditability.

Procedures that ensure that the above or any other actions are traceable, auditable and demonstrable through the generation of digital evidence.

8. Intuitive system with feedback

CRANE model should be made thinking about the accessibility of chronic patients by incorporating digital and health literacy tools in the system. Self-instruction videos, a feedback system that demonstrates gains for the individuals and explainers can be considered to understand how to correct self-monitoring procedures are performed. Other sources of information such as FAQ sections, chat boots and telemedicine call centres shall also be considered.

4.3. Other Technical Data Requirements

CRANE should be based on a **digital open platform** (or a systematic integration/combination) with the capacity to:

- Integrate: existing and next appearing monitoring sensors and/or devices for intervention in the different pathologies addressed (monitoring, rehabilitation …), communication mechanisms among participants, and increased safety of customers.

- Communicate: to enable the integration of all activities in a continuous care path centered around the patient; communicate with existing IT systems from all participating stakeholders for data sharing,
- Enable data management: The scope is to create a customer-centered data model for tracking and visualizing regional service utilization, costs/resources and effectiveness in order to create value for both citizens/patients and the involved organizations/partners.

The enabling technologies that could be included in CRANE to address the proposed objectives are:

- Tools for anonymisation and pseudonymisation.
- Secure Multiparty Computation (SMC) for sharing secrets (PII).
- Blockchain for both storing and managing informed consents, considering the ENISA recommendations on access control to the stored information.
- Different encryption methods and algorithms for private information data processing. For instance, the Computing on Encrypted Data could be related to the new research activities on homomorphic encryption.
- Governance tools for managing and monitoring repositories, infrastructure, access control, logs, backups, …
- Data Privacy Impact Assessment (DPIA) and security measures and security policies and guides in different items like AI and Machine Learning.
- Integrated proposal for all the functional requirements and technologic requirements.
- Interoperability layers
- Intuitive software for chronic patients

Depending on the specific provided system, the following technical requirements may be then of application:

1. Artificial Intelligence Framework

Development of an ethical impact assessment of AI in case of including specific AI services or using the data of the repository for the development of AI tools.

The High-Level Expert Group set out a non-exhaustive Trustworthy AI assessment list to operationalise Trustworthy AI. It will be recommended to the developers to take it into account during their ethical evaluation. The tool "Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment" could be used to implement this assessment.

Moreover, in case that AI is related to Machine Learning, the ENISA guide on "Securing Machine Learning algorithms" should be considered.

2. Secure Multiparty-Computation SMC: anonymisation

SMC could be conceived as a supplementary measure and potential data anonymization tool. The anonymisation in CRANE could potentially be developed applying the recommendations of the Opinion 05/2014 on Anonymisation Techniques (0829/14/EN/WP216). And, in case that SMC is to be used, also the recommendations from ENISA in the report "Data pseudonymisation: advanced techniques and use cases".

4.4. Other transversal requirements

In addition, and depending on the type of the provided solution, the following transversal requirements may be of application to the provided solutions:

1. Training staff

On data protection law and its basic principles as well as into the subjects who must categorise and classify the information that will subsequently be accessible.

2. Supplier requirements

Identify the requirements accessible to external suppliers if their services are required. In particular, and irrespective of their role (processor or joint controllers), particular attention should be paid to defining the reliability requirements of suppliers of software and hardware, cloud computing, data analytics and ai applications, mobile applications and analysis, development and/or programming services

3. Identify additional requirements of the platform:

- Application processes for data access, design of specific data analysis and access to results of data processes executed by the platform
- Administrative management tools (ticketing and process management).
- Procedures for user registration/discharge and acceptance of terms and conditions.
- Procedures for formalising commitments: data-sharing agreements, ethical commitments and non-reidentification commitments

4.5. Other Applicable Regulations

The following table collects a short list of the key potential regulations that we believe could be of application to the CRANE proposed developments.

Required Regulations and certifications	CRANE 3rd party data sharing (MyHealthEnabler) provider	CRANE Data Service providers
ISO 13485 - Quality Management System **Company/Consortium Focused**	If applicable the Platform suppliers will need to comply with MDR. If so they need to document its plan for compliance with support services for the Service provider's devices and/or automated processes.	Service providers should ensure that all devices and automated processes comply with ISO 13485 when going to the market commercially. Service providers should document or obtain from device suppliers all certification documents
ISO IEC 27000 Standards family on Information Technology. Security **Company/Consortium Focused** **Software development** **System communications**	Cyber security should be assessed in all areas of the regulations the above and below standards should incorporate the needed documentation for the various security components, the bidders should need to ensure that all components are identified and documented to the appropriate level. Furthermore, it includes special standards on systems based on cloud (ISO27018), privacy	Cyber security should be assessed in all areas of the regulations the above and below standards should incorporate the needed documentation for the various security components, the bidders should need to ensure that all components are identified and documented to the appropriate level. Furthermore, it includes special standards on systems based on cloud (ISO27018), privacy

	requirements (ISO27701) and certification (ISO27001).	requirements (ISO27701) and certification (ISO27001).
ISO 14155:2020 - Clinical Evaluation Process **Company/Consortium Focused**	If applicable, the platform provider should supply supporting documentation to demonstrate expected software development practices	If applicable, Service providers should follow the process with an acute understanding of the need for effective root cause analysis (RCA) and corrective and preventive actions (CAPAs) for significant non-compliance as well as for device deficiencies throughout the conduct of clinical trials.
ISO 14971 - Risk Management **Product & Services Focused**	The platform provider should supply all applicable supporting documentation such as audits and error logs as needed for service providers to maintain effective risk documentation	Service providers should ensure all appropriate documentation for tracking the risk of devices and services following ISO regulations
IEC 62304 - Software life cycle **Software Focused**	Platform providers should supply supporting documentation to demonstrate expected software development practices	The service provider should supply supporting documentation to demonstrate expected software development practices
IEC 82304 - Software life cycle **Software focused in an open environment**	The platform provider should supply supporting documentation to demonstrate expected software development practices	The service provider should supply supporting documentation to demonstrate expected software development practices
IEC 62366 - Usability **Software Focused**	The platform provider should supply supporting documentation to demonstrate expected software development practices	The service provider should supply supporting documentation to demonstrate expected software development practices

Table 4. Regulatory framework for CRANE

5. Pre-commercial procurement (PCP)

Pre-Commercial Procurement (PCP) is an approach where the public sector challenges industry to stimulate the development of innovative solutions tailored to its need. It helps public procurers to develop the required solutions filtering the best possible solutions that the market can provide. CRANE will use this approach to addresses the comprehensive treatment of chronic conditions in rural areas.

5.1. PCP Process

Phase 0. Research and development

This phase includes all the necessary steps to prepare the first Call for Tenders. In the case of CRANE: workshops, bilateral meeting between procurers and providers and four Open Market Consultations

(one per each region involve in the project and an international one). These actions carried out during the first months of the project allow CRANE partners to have insights on the market needs and define the specifications and requirements of the solution. At the same time, CRANE partners reviewed the actual knowledge on the area and started a technical dialogue with the industry to ensure the success of the call and that the solution is ground-breaking.

Phases 1 to 3. PCP execution

During PCP execution different suppliers will compete in parallel through different phases of development to find solutions to the CRANE challenge. It will consist of a joint PCP procurement where procurers buy R&D from several suppliers that compete in parallel. This stage will start with the publication of the call for tenders, that will remain open for at least 60 days, followed by the evaluation, awarding and stand-still period. The full action consists in a 3-phases competition with the number of competing R&D providers reduced after each evaluation phase. In each phase PCP contracts are assigned under the supervision of the buyers' group.

PCP opens the route to the market for new players and also allows to compare different solution approaches. This will identify the best value for money solutions that the market can deliver ensuring execution of the R&D services by the providers according to the action plan and requirements defined in the preparation stage.

Process Phase 4. Public procurement of innovative solutions

This stage aims to facilitate wide diffusion of innovative solutions on the market. It will start right after the end of CRANE to translate the results of the project to the market.

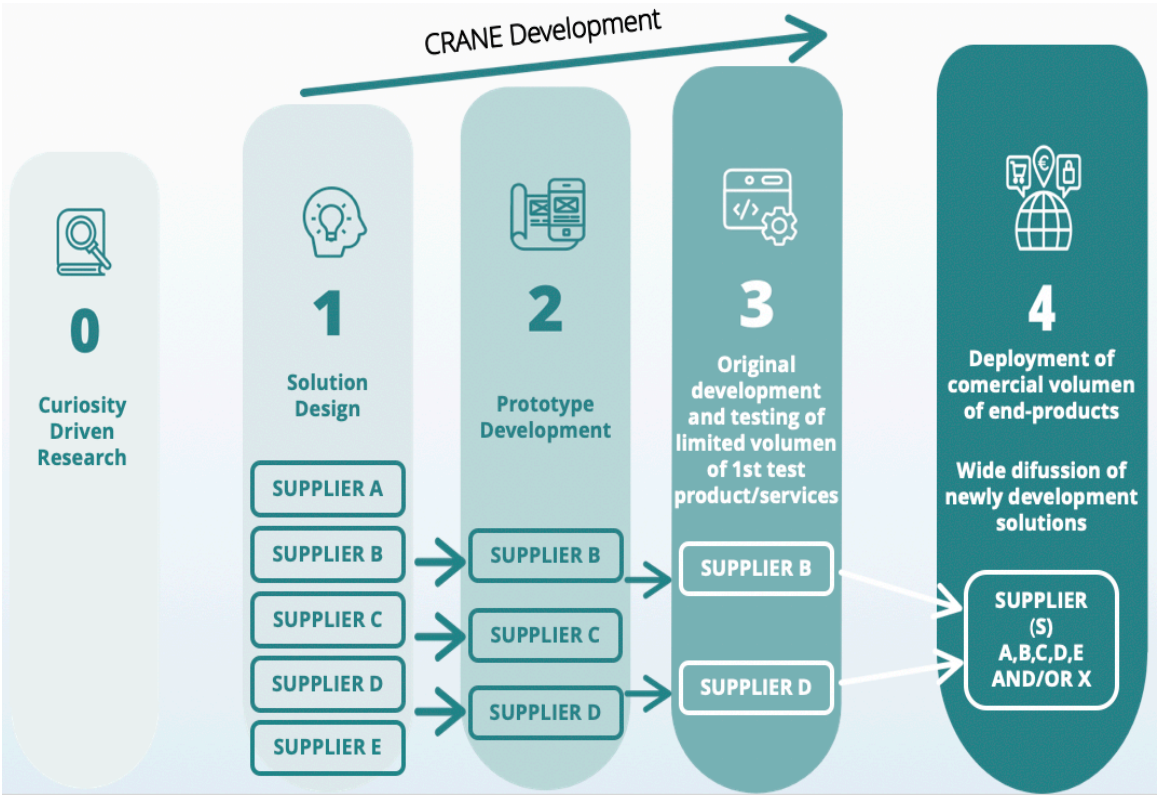


Figure 4. Pre-commercial procurement phases

5.2. CRANE PCP key data

CRANE will launch its Call for Tenders in Summer 2022. In Phase 1, we will invite five bidders with 50,000€ budget each for the development of a feasibility study. In Phase 2, each of the three selected proposals from Phase 1 will get 500,000€ to develop a Prototype. Finally, in Phase 3 two suppliers will be selected with 1,45M€ for a Field Testing.

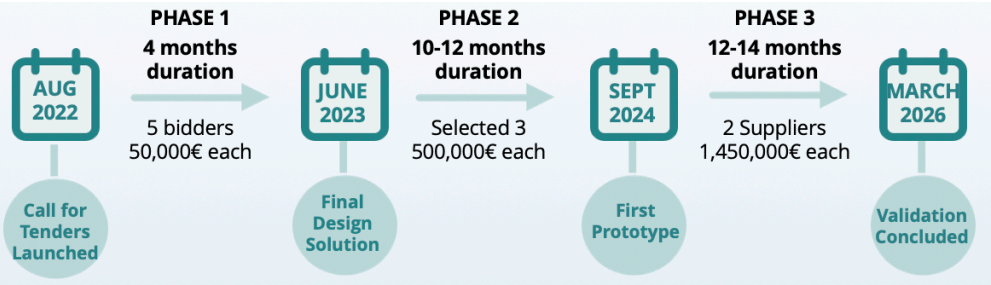
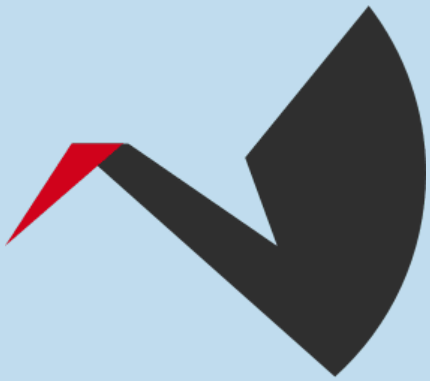


Figure 5. Predicted timeline for CRANE PCP execution



CRANE

Comprehensive treatment of chronic patients in rural areas

region västerbotten

C3 Centre for Connected Care

EUROBcreative
Intelligence on the move

JUNTA DE EXTREMADURA
Vicepresidencia Segunda y Consejería de Sanidad y Servicios Sociales

PPCN
Making impact & change

REGIONAL COORDINATION GROUP
E-HEALTH AND WELFARE TECHNOLOGY
AGDER

VALDE INNOVA

Funded by the European Union

This project has received funding from the European Union´s Horizon 2020 research and innovation programme under grant agreement No 965277