Interreg CENTRAL EUROPE
European Union
European Regional Development Fund

niCE-life

ANALYSIS OF THE STATISTICAL DATA AND INTEROPERABILITY OF DATA

Deliverable D.T1.2.3 **version 1.0**

Content

Executive summary

Within the output, individual documents from partner countries were processed on the basis of processed needs of target groups. Following the evaluation of this data, a procedure was developed to ensure interoperability requirements for each digital tool. There are large differences between partner countries in terms of hospitalization and post-hospital management. Long-term and repeated hospitalizations are ideal for using digital tools from the perspective of ensuring continuity of care. From this point of view, it is important to digitize the process in order to facilitate data sharing. Good e-Care practice has a huge advantage over other project partner countries in that it uses fully digitized EHR (Electronic Health Record) documentation. High efficiency of data sharing is also ensured by the fact that the principle of providing nursing and social care operates under one common ministry, which enables better coverage of care from the perspective of health care payers. As a result of the above, it is worth mentioning that what is good practice in Bologna is not a form of EHR in other countries. The digital tool for patients discharged from hospitals responds to this, when there is a need to share data between private health and social service providers, when often not all the necessary documents are available to ensure quality care. This issue is especially common for Central European regions, where there is also the absence of strategies that would address the electronic document. The region of Emilia-Romagna has had a specific law for the integration between social and health assistance addressed to persons with disabilities and elderly. The Regional Government established taxes with the aim to create a fund. This integration promotes the involvement of private organizations accredited by the public for the provision of services. This is to some extent due to the fact that in two of the 6 partner countries, Beveridge has a healthcare delivery model, while in the rest of the countries the Bismarckian model is applied. There is a great difference between the project partner countries in terms of the involvement of individual regions in the issue of adoption of innovations at the level of health and social care. In individual strategies focusing on health and social care in the given regions, the mention of eHealth is often only marginal without any deeper concept.

The large number of digital tools has the disadvantage that, on the one hand, certification is required for use in healthcare, but in many cases the effectiveness from the point of view of health insurance companies is insufficiently proven. These digital instruments can sometimes be reimbursed from private insurance.. In social care, a common feature is the use of technology in that clients buy these solutions from individual private service providers such as panic buttons. The problem with these solutions is false reports, where patients, especially with mental health problems, overuse it excessively due to psychical conditions. From this point of view, it is therefore necessary to involve the patient as little as possible in the entire monitoring process in his natural environment. According to their needs, seniors partially control video consulting tools, where they are taught to use them, as they are used to communicating with their family members in this way.

During the Covid pandemic, video-consulting tools were widely used, as there was often no other way for social contact but also with liaison providers. It is necessary to take into account that most of the

tools that are currently created are for the generation that already owns a smartphone / tablet or computer and has a foundation in digital literacy. It tells about the current situation of the technologies used and their frequency among seniors is a questionnaire survey prepared by LEPIDA and from which it is clear that most of the information that seniors obtain from TV and newspapers. The questionnaire survey was performed on two groups of patients based on the frailty index. The lower the frailty, the more seniors use digital tools.

From the interviews it is clear that the experience with digital tools is only very marginal and mostly without any other concept in terms of organizational, economic and clinical aspects. Digital tools are designed as a solution that can be integrated into existing systems via an open API or can run in parallel with existing systems. The project clashes with digital solutions, which are often at the crossroads of health and social care, and from this point of view the integration of processes is more complicated, given that some countries do not use EHR. In most cases, it was a requirement from seniors to feel safe and would welcome technology if they were helped with it. Most often, they also expected that technology would increase their quality of life and at the moment when their lives were endangered or at the moment when there was a continuous deterioration of their health, which could result in hospitalization.

An important role from the point of view of risk analysis was the involvement of family members in the care of their loved ones. It is about informing both clients and family members about what services can be used and what are the criteria for assisted living, including the definition of what services are included and can be used. For clients over the age of 65, family members are interested in their current mental and physical condition. To this end, a Monitoring Grid tool was designed using the so-called frailty index, which will be used by the Austrian partner and will also be part of the platform for seniors discharged from the hospital, which will be verified in Slovakia and primarily in the Czech Republic.

The output used a methodology where a template was created based on the methodologies MAST (Model for assessment of telemedicine) and Momentum (Moving telemedicine from pilot to scale 18 Critical Success Factors), where individual partner countries answered structured questions about the digital tool. These questions were focused on the description and differences of individual health and social ministries from the point of view of providing care. Subsequently, based on the Momentum 18 Critical Success Factors, the questions were adjusted and the differences between the individual partner countries were monitored in terms of readiness for the adoption of digital tools. Each of the partners then worked out the needs and barriers from the perspective of 7 basic groups. Then, individual interviews were conducted with the recipients of care, and their needs were analysed.

Introduction

This document has been created within Deliverable D.T1.2.3 - Analysis of the statistical data and interoperability of data. The purpose of this deliverable is to do an evaluation of statistical data obtained from the need's assessment (A.T1.1) and consideration of interoperability of input data flowing to the health and care monitoring platform. The aim of this document is to describe what are the common needs of frailty people who suffer from chronic illnesses. These needs are summarized in first part of the document. In its second part is summarization about interoperability focused on data security (authentication, data protection, security monitoring, safety, data storage via cloud, functional requirement, data sharing etc.).

As been mentioned above Output D. T1.1. 3. is based on reports on needs and current practices at regional level in each partner region. Main aim of this output is to describe current practice from the perspective of possible improvements in methods and approaches and also to think about the possibility of moving the individual functional measures in the context of care for the frail elderly between partner regions. Based on inspiration, to suggest possible solutions to problematic areas for further elaboration and adjustment for local conditions.

The outputs provided by individual partners serves as supporting materials. Thanks to the reactions of our partners, we are able to try to define the main problems concerning fragile seniors and also how they can be solved.

It should be mentioned that each region faces one and the same problem, which is called demographic aging. Information about the increase in the number of people over the age of 65, but especially also the number of people over the age of 80, was heard from each of the partners. However, the way of working with these people is different from the social and health point of view in each country.

The issue of healthy aging in modern society is interest in the field of science and research, also in the field of medicine, biology, social sciences and technical sciences. The urgency of solutions in countries where the population is aging at a relatively fast pace should lead to practical solutions that we believe will emerge from the niCE-life project. The pace at which states prepare for demographic aging, which sociologists reported long ago in the last century, is not appropriate or enough. As an example, we can mention the regular conference entitled: "Education and work in the 3rd age - an opportunity for society". This is already the 9th annual conference, so we ask the rhetorical question when education in the 3rd age will cease to be an opportunity and will finally become a reality?

Analysis of the statistical data

Hospitalization

Hospitalization does not only mean high costs of care as stated. Good example is Poland, which is trying to reduce the length of hospitalization of seniors but far not very successfully. The Czech Republic also places emphasis on shortening the length of hospitalization, and the economic reason is also the main reason here. However, the Czech Republic is doing well, mainly due to pressure from health insurance companies. Insurance companies create obstacles for reimbursing long-term hospitalizations, and hospitals thus know that long-term hospitalization is economically disadvantageous.

Italy describes beside high costs as the reason for shortening hospitalizations also another reason. It is based on the assumption that the longer a senior is hospitalized, the more follow-up care he will need and the more difficult it will be to return to the natural environment. Austria is aware of this benefit and is gradually taking it over. This is an idea that the regions should embrace as a challenge – to do not shorten hospitalization for economic, but mainly social, psychological and health reasons.

From the ecomonic point of view, in Poland and Austria it is possible to take out additional private insurance, which causes problems especially in Poland in the form of unequal access to health care. In Poland, there is a separation between private and public hospitals. Wealthier seniors who are subsidizing private insurance can get for example total hip replacement significantly faster, than seniors eligible for health care under the statutory insurance. In Austria and Slovenia, there is also supplementary insurance, which, however, tends to cover increased costs beyond ordinary insurance.

Data sharing

The problem of "data sharing" is closely related to hospitalization and care for the elderly. In most of regions, healthcare is apart of social care. Good practice is taken from Italy, where certain data are shared: "The Municipality of Bologna and LHA BO share data resulting from application of the index with Lepidus and social stakeholders, in particular to protect older people ..." Mayors here take part of responsibility of heatlh of population and share data on care for the elderly with eCare services. Then, eCare operators call seniors and inform the services to obtain a privacy consent form. The model of caring for people in need in cooperation with many actors should be a matter of course. However, even Italy itself, which has high level of electronic communication and support in government organizations and laws, admits that "the level of integration between health and social care is still low from a political and organizational point of view".

Austria is also further in sharing data than other partners. It has a system called " ELGA - elektronische Gesundheitsakte " developed between 2006 and 2010 and is to be implemented gradually from 2015 to around 2022. Access is managed and controlled through an electronic card system. The HL7 standard forms the basis for data access. Patients have the option to log out to restrict or prevent use. Through ELGA, facilities such as hospitals, general practitioners as well as pharmacies and care facilities are interconnected.

The problem of sharing and possible computerization of data is especially noticeable in the Czech Republic, where the system is slow and places greater demands on the cooperation of the patient, health services, social services, GPs and all documentation still takes place mainly in paper form.

For other partners, the situation around the electronicization of data in the field of healthcare is closer to the level of the Czech Republic, where the electronicization of medical records, etc. is at a low level. It is necessary to realize that the change in this area is not only linked to the technical solution and the fulfillment of the requirement for GDPR, but it is also necessary to think about the legislation in the countries of individual partners.

In Poland, the problem of sharing data between the health service and social care requires an authorization from the Senior in the online patient account (IKP).

However, we agreed on the fact that data sharing between individual actors is one of the key situations that partners should address and be inspired by the individual steps taken, in particular, by Austria and Italy.

Care for the elderly and assistance of other actors

Population aging and other immediate demographic challenges call for a new type of intergenerational solidarity. Today's average family lives apart from its older relatives, the frequency and quality of communication between the generations is relatively limited, and therefore it cannot itself bear the burden of caring for elderly family members. Older people generally wish to stay in their home environment until they die, or at least for as long as possible. Slovenian, Czech and Slovak data show that elderly decide to go to social facilities due to fears that they will become a burden on the family and because of lack of various non-institutional solutions .

The willingness of the family to care is relatively high. The most common motives for care are emotional ties, a sense of duty and moral responsibility. The biggest problem is not the willingness to care, but rather the ability to care, economic loss, disruption of private life and length of care.

It is necessary to realize that as life expectancy increases the caregiver himself is often over the age of 70.

A possible solution is to combine public care services with services provided by non-profit organizations, informal carers and private care.

A survey among family carers shows that their needs differ, but they still have some in common and these are repeated with other partners, such as the Czech Republic, Poland, Slovakia. Caregivers mention in particular the needs of respite care, which are insufficient and relatively expensive in Slovenia, but also in the Czech Republic. They would also like "more frequent visits by the district nurse" and "greater availability of home help services". Other expressed are needs of recognition, support, help of other family members, as the most often caring person is a woman - wife, or daughter.

Here we can see the possibility of introducing telemedicine as a supportive tool of care for the elderly in the home environment. The possibility to consult the state of health, entering measurable data, etc., which would save the demands to travel with the patient for doctor's appointment would certainly help, as well as share your concerns with a psychologist, etc., which in not possible in case of single carers.

In the Czech Republic - Olomouc, joint meetings of carers proved successful. Family caregivers shared their worries and problems while outpatient service took care of their love ones. Family caregivers was thankful mostly for the time for rest.

It is necessary to realize that caring for a loved one is very time consuming, often without proper rest seven days a week. Healthcare can prolong a senior's life quite significantly, which results in a disproportionate long-term burden on the caregiver.

Services for the elderly in the household

All partners agreed on the fact that seniors who are at home and relatively able to take care of themselves, but already fall into the category of fragile seniors and often have trouble leaving the house, for example, because they live in an apartment that is barrier and they can't easily come out.

Surveys show that seniors most often spend time watching television, feeling lonely and prone to depression, which in turn causes other health complications.

Contact is very important for seniors. It cannot be replaced by the best application, but at least a human living voice could help.

Almost all partners have a form of emergency care services, call centres, which from time to time call the senior with a question about his condition. Some of them have a technique that monitors the movement of a senior around the house, can be connected to a wearable technology with fall detection, or. inactivity, etc.

However, this service is at a different level in the case of Italy and Austria, which were inspired by Italy and are the furthest in the solution within the partner countries. Italy has created a kind of fragility index with which it works, and which monitors the development of seniors over time and can predict the need for hospitalization, etc. The monitoring grid, which is based on the practice from Italy, Austria adjusts is exactly the transferable practice between project partners. Other countries do not have such a well-developed method and only one of the countries works more with the fragility index and uses, for example, the Barthel Scale , which is not very suitable because it cannot work with mental problems, such as dementia.

Seniors and modern technologies, possible solutions

A frequently mentioned fact across partners is the generally lower ability of elderly to master modern technologies, and there is also a relatively large intergenerational gap. However, seniors often have, for example, a smartphone, but less so a computer with an Internet connection.

It is appropriate to train seniors in working with ICT, for example, during preparation for discharge from hospitalization and to pay attention to the education of seniors in ICT in general.

The practice presents a possible solution where chronic patients (chronic obstructive pulmonary disease and chronic respiratory failure, chronic heart failure, amyotrophic lateral sclerosis, after a stroke and after cardiac surgery) are admitted to a program that offers telemedicine services after a period of rehabilitation in the hospital. The Telemedicine service consists of structured telephone support and telemonitoring managed by a doctor and a nurse. An educated medical team is involved, including specialists, nurses, physiotherapists and technical staff. A key role in the service is played by a nurse-lecturer, who connects all hospital and domestic staff by telephone. The intervention consists of four main components:

1) educational events before discharge about the disease and its therapy

2) regularly scheduled telephone coaching

3) home telemonitoring of various parameters (weight, blood pressure, heart rate, saturation, etc.) in real time and evaluation of scales that will help patients detect worsening symptoms,

4) If necessary, the second opinion of a specialist for the patient's nurse or general practitioner. The equipment supplied for remote telemonitoring depends on the main problems of the patients. If rehabilitation sessions are available, a video conferencing solution is provided.

A practise is focused on allowing person use omnipresent and non-stigmatizing consumer technology in preventively way, prevent a negative incident and help them to stay independent longer.

The aim is to use the potential of technology to improve the quality of life and save money from public resources, by changing the way the care is provided, increasing the independence of seniors and reducing the number of hospitalizations.

The system, when a call centre just don´t call for question – how are you today, but try to solve more complex structure of question, which can aim specifics findings connected of fragility, risks of fall, grip strength, muscle mass, level of hydration, etc. All this information can be following and measure from everybody´s home using the latest portable technologies. The obtained information helped to identify a lot of indicators of fragility, which were without attention, for example user of social care, who can be dehydrated, have a low pressure, risk of fall, etc.

However, a big problem is a group of physically fit seniors with a higher degree of dementia or Alzheimer's disease.

Interoperability of data

Following requirements are intended as a guide of minimum cybersecurity measures in the organisation for taking adequate cybersecurity and data protection risks.

Although this is not necessarily a complete list of security measures and it is possible to introduce other measures beyond those listed below, the security measures listed for this standard are given as a minimum.

If an organisation is unable to meet these measures to meet the sensitivity of the information provided, the security level of the application needs to be reduced by changing the content and sharing sensitive data in other secure ways.

The criterion for the protection of communicated information, which is required by law, contractual arrangements or other regulations, is based primarily on the obligation of employees to maintain confidentiality about facts they learned during their employment (generally the Labor Code, the Administrative Code, or other special legislation) or from the obligations that bind the organisation due to the content of the contractual arrangements.

Data security

1. Authentication

   1.1. Use the central administration of privileged accounts (LDAP, MS AD, etc.)

   Implementing central administration of privileged accounts reduces the risk of unregistered accounts being created, changes not being recorded, and if the reason for the account's existence ceases to exist, the account is not invalidated, and there is a risk of abuse, for example by a former employee. At the same time, the risk of breaching their confidentiality increases with local accounts, especially in the event of insufficient control and security settings on the device.

   1.2. Use central management of user accounts (LDAP, MS AD, etc.)

   Implementing central user account management reduces the risk of unregistered accounts being created, changes not being recorded, and if the reason for the account no longer exists, the account is not revoked, and there is a risk of abuse, for example by a former employee. At the same time, the risk of breaching their confidentiality increases with local accounts, especially in the event of insufficient control and security settings on the device.

   1.3. Enforce credentials and their complexity

   Sufficiently comprehensive verification data, resistant to brute force attack, must be enforced for verification. The following **recommended** rules apply to user accounts:

   - the minimum length of the password is 10 characters,
   - ban on using the same password (last 12 passwords),
   - the maximum validity period of the password is 18 months,
   - account lockout after 10 invalid password attempts in a row,

- a one-time initial password that must be changed after the first login or revoked after 24 hours.

These rules must be understood as minimum recommendations and their implementation may be stricter.

1.4. Use multifactor authentication

For authentication, it is necessary to use multifactor authentication (electronic key, mobile key, authentication item, etc.), especially in the case of authentication of privileged administrator accounts.

If mechanisms based solely on shared knowledge (name, password, e-mail, PIN) are used for user authentication, it cannot be ensured that this shared secret (authentication system and user) cannot be used without the user's knowledge. There are a number of threats (surveillance, eavesdropping, intentional or unintentional recording, disclosure, etc.) that can misuse this data. In contrast, multifactor verification is based on a combination of at least two of the following three types of factors: 1) ownership of a physical object (a card, token, random code generator tied to a specific object), 2) knowledge (PIN, password, etc.) or 3) biometrics.

1.5. Use SSO authentication

It is used for SSO (Single Sign-On) authentication on a secure device. Authentication to the system is performed on the basis of trust in the already performed user authentication, user account against the central IdM server (e.g. LDAP or MS AD).

2. Access control and protection of personal data and processed data

2.1. Separate roles

Setting permissions for the administration and operation of the system is implemented through assigned roles. The authorisation is not assigned directly to individual accounts. Roles are separated so that it is not possible to assign and use permissions under one and the same account.

2.2. Integrate the role management process with existing IdM

To assign individual roles to specific user accounts (creation, changes and deletion), a secure process is set up, including registration and approval procedures, so that unwanted authorisations are prevented and all authorisation management activities are recorded. A specialised IdM (Identity management) system is used to manage these processes.

3. Security monitoring

3.1. Manage and evaluate security logs

The solution must enable the collection of security audit records (logs) to the required extent, based on the requirements of legislation and best practice. These are mainly the areas of authentication, authorisation, accounting, key management and certification services. Critical operations (multiple login attempts, etc.) must be monitored and reported.

3.2. Evaluate application logs (set-up, user connections)

The solution must enable the collection of application logs about the activities of administrators and users. Records must be available to the organisation to the extent required based on security requirements. It must reflect the history of how the protected data. Best is to connect system to log management or SIEM.

3.3. Audit security settings

The system in an organisation must also include an audit of security settings or procedures and their compliance. The audit is performed at regular intervals and during changes that may have a negative impact on the security of the system. In determining the frequency of the audit, the nature and extent of the risks and impacts associated with the operation of the system should be considered.

3.4. Connection of video conferencing system to DLP solution

Use the DLP data protection system when transferring text information or files containing protected information.

4. Cloud requirements

4.1. Ensure the requirement to store data in the EU

The storage of customer data must be within the jurisdiction of the EU. This applies in particular to cases where it cannot be guaranteed that the data is securely protected by enterprise-wide encryption and is not stored in the cloud during transmission, even temporarily. The conditions of the GDPR for the transfer of personal data must be met, in particular Articles 44 to 49 of the GDPR. In the case of transmission of communicated information or metadata, the organisation must be informed where this data is transmitted, for how long, for what reason and to what extent

4.2. Document ISO / IEC 27001 certification

Because the organisation does not have the ability to directly affect the security of the cloud solution provider or the services it provides, the level of security by the supplier must be documented. Confirmed proof of compliance is best used for this. Therefore, the organisation must require the supplier to hold a certificate proving compliance with the ISMS management standard, ISO / IEC 27001. If the vendor is not ISO / IEC 27001 certified and the security level of the videoconference corresponds to this, the organisation must require the vendor to provide an appropriate equivalent (for example, an SOC II Type 2 audit report or otherwise provide an on-site audit).

4.3. All communication (if possible) must take place via trusted servers

As part of a solution where the organisation does not have control over all the components through which system is conducted, it must verify that communication within system is conducted exclusively through trusted servers from a trusted vendor.

4.4. The transmitted data shall not be permanently stored on the intermediate device (s).

The transmitted data must not be permanently stored on the devices mediating the transmission. When temporarily stored, they must be adequately protected and this must only be for a limited, clearly defined period of time.

5. Additional safety recommendations

5.1. Do not use unsecured public networks (WiFi hotspots) for external system connections

Unsecured WiFi networks can be sniffed by an attacker who can steal sensitive patient data or who can connect to this network to performed same attacks e.g. ransomware, which can cause a denial of data of stations inside the network.

5.2. Implement DoS / DDoS protection

DoS (denial of service)/DDoS (distributed denial of service) attacks are quite often on cloud services or servers with many active users. These attacks will deny connection to all of the users to the server. To protect against DoS/DDoS attacks on cloud servers, we need to use additional special servers which will control and evaluate incoming network traffic and drop infected connections.

5.3. Ensure infrastructure redundancy, load balancing

The infrastructure of the cloud needs to be well designed. If the same server of cloud would fail, we need to have a redundant server to ensure standard cloud functionality. Load balancing is the way how to balance high network traffic from one source to all parts of the cloud not to occur overloading of a single part of the cloud.

5.4. Perform infrastructure testing against outages

Before the cloud is deployed online for real usage, we need to perform testing against outages or failures. If some part would fail, the cloud must be extended with appropriate hardware to prevent this outage.

5.5. Perform and evaluate penetration tests, DoS / DDoS tests

To ensure that the infrastructure of the cloud is created appropriately, some penetration tests or DoS attacks need to be performed. This penetration tests can be performed by us or, e.g. with an external company focused on security testing. After testing procedure, we would find vulnerabilities and secure them. Further, we would find the maximal number of servers performing DDoS attacks,

where it is possible to have cloud stable. According to this result, we can increase the capacity of servers in the cloud and add additional servers for detecting DDoS attacks.

5.6. Requirements for the security of cloud services must depend on the level of service provided (SaaS, PaaS, IaaS)

- SaaS (Software as a Service) - it can be on-demand software that can be used.
- PaaS (Platform as a Service) - allows users to developed and run their own applications.
- IaaS (Infrastructure as a Service) - provides users API for using network infrastructure resources or services.

Security requirements would be according to the selected system.

5.7. Require the cloud service provider at least the same level of security as when conducting a system with the company's own resources.

Selected cloud service must be at least at the same level of security as systems of all core members and their sensitive data.

5.8. Require the same level of security for all subcontractors whose activities may affect the quality and security of the system provided.

Fundamental security rules provided must be valid for all parts, including subcontractors, to prevent data leakage or other failures.

6. Functional requirements

These requirements define the scope of the service and its applicability. The aim is to define the balance between security and usability of the service. The basis of service security is unquestionable authentication of the user and management of his access rights. Identity verification is a key security parameter for solutions provided in public cloud services. Requirements for its complexity are given by the required security level and requirements for the management and protection of identities.

We define as basic functional requirements:

- Interoperability - a cross-platform solution based on open standards (European Communities (2004), European Interoperability Framework for pan-European eGovernment Services)
- Authenticated and external approach - proving the identity of users tied to rules and technical measures; access control and roles based on user identity. Possibility to control access of external users
- Communication channels – default and optional pathways used for distant communication (sharing of health data, conversation, content sharing, ...)

- devices and other technical equipment - requirements for technical equipment used by users
- Protection of transmitted data - system architecture and protection mean
- Protection of stored data - system architecture, DLP against unwanted disclosure of information by the user

- System management - ensuring a safe and trouble-free system is operable
  - Integration - the interconnection of digital communication and data exchange based on open industry standards
- Monitoring - online supervision of the system
  - Reporting and audit - historical reports, including user and administrator activity

7. Information sharing

7.1. All participants can share the following types of information

- EMR(Electronic Medical Record)/her(Electronic Health Record), Files (documents)
- Notes
- Other personal and optional data (GPS, calendar records, etc.)

All data and information generated during data exchange and transfer (see above) must be transparently stored and wholly owned by the organisation. The organisation must be able to manage and limit the storage of data in selected geographical regions, primarily the European Union (EU) and the European Economic Area (EEC). Data access control is required. Essential prerequisite for sharing of the data is compliance of the participant with GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)) and patients´ consent.

7.2. API

Application interfaces offer integration options beyond ready-made applications or plug-ins. For example, you can build a planning system with advanced features or build a data exchange system on existing workflows. However, the API offers both user and administrator functions, so it is necessary to pay attention to its security. The essential security parameters of the API are:

- Use of secure protocols with an appropriate level of cryptography
- Configurable security by systems policies

- Modern methods of authentication and authorisation, which will allow:
  - Determine the range of services available for a specific application
  - Do not store usernames and passwords for API access in the application
  - Block the application from accessing authentication information
- Communication API logging

Interoperability of data

The aim of interoperability is mutual interaction between project partners to achieve beneficial results including the sharing of data of their ICT systems and their knowledge.

The project partners involved in the project have possibilities to use the data from patients in order to gain comprehensive insight regarding the overall trends and better understand the current situation. Here more data means more information that can be extracted. The overall scheme of selected project partners and their contribution is provided in the figure below. BUT will contribute with the intelligent monitoring tool and will work with sleep patterns. SAM, LEPIDA. UHO will gather feedback regarding the health status of patients and will visualise metrics that will be computed based on questionnaires. This follows good practice taken from LHA BO project partner.

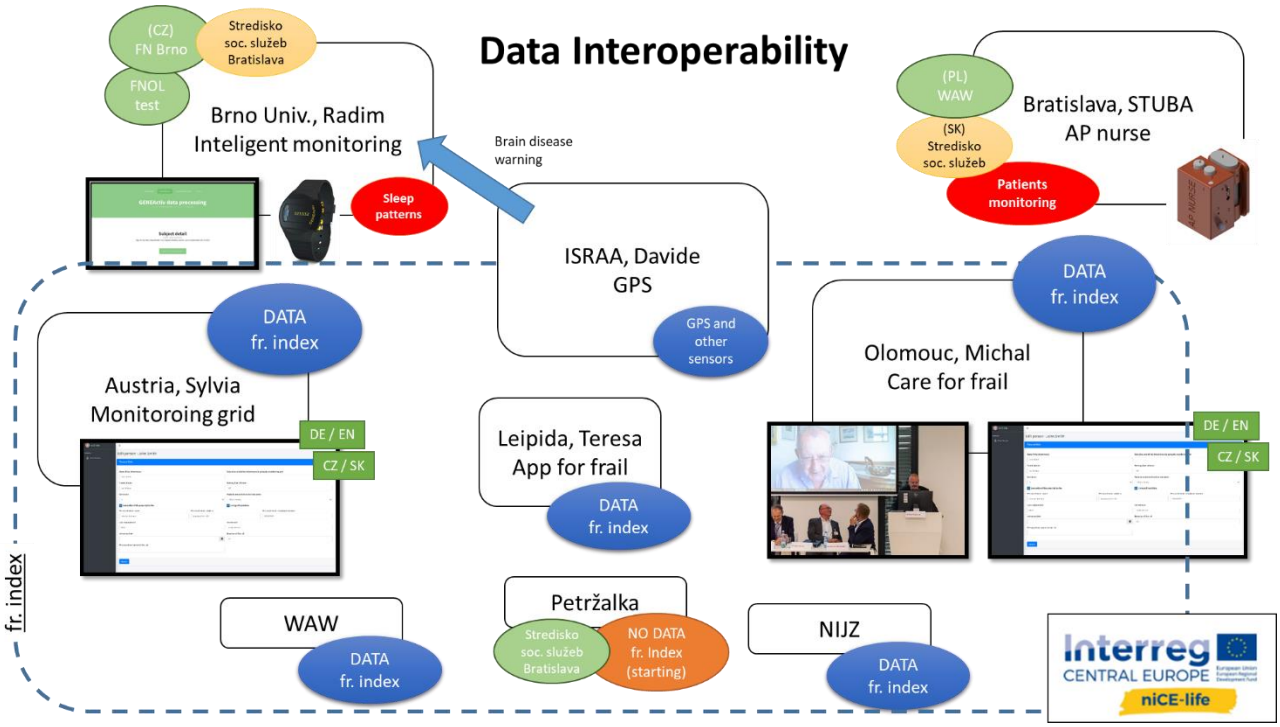


Figure 1: Overall scheme of project partners and their contribution to the project.

Each project partner will use a different way to collect data that contains various information. Data can be obtained with using intelligent monitoring (smartwatches with sensors, monitoring devices for patients

discharged from hospitals, standalone non-medical sensoring devices, questionnaire app for frail) or from EHR/EMR. The aim is to collect data into global safety storage and have them accessible for all members. The prediction system will use these patient data, and it will predict e.g. patient state in the future.

Overview of the data the participants can contribute to data interoperability are described in the table below:

Proj. partner	Task name	Data type	Data Description	Interoperability	Data analysis
Petržalka	Participating to other tasks T1.2, T1.6	Starting collecting data regarding fr. index	There is plan to start collecting data regarding frailty index.	Institution is about to start regularly collect and evaluate data. Unfortunately, today the data are relatively limited.	Expected contribution regarding frailty index. Since the institution is starting with data collection, data are expected to be possibly limited
BUT	Intelligent monitoring tool	Time series, sleep patterns	Time series regarding sleep patterns and early detection of Parkinson disease. These data differs to other data sources significantly and are not suitable for any interoperability to other applications.	Due to sensitivity nature of the data there is not expected to use the data for interoperability and further analysis	Yes - machine learning of sleep patterns
UHO	Care for frail	Tabular data - frailty	Questionnaires evaluating frailty index of people, monitoring health condition and trends in time by IEEE 11073 / Continua Health Alliance Standards compliant devices when available. Videoconference platform for consulting with doctor	Questionnaires and frailty index based on metrics could help future analysis of trends and patterns in health conditions	Analysis of pneumonia Analysis of frailty index

STU	AP Nurse	Time series,	Data related to electronic devices, which are related to safety of hospitals. These data are unfortunately not labelled and differs to other data sources significantly. Ddata transfer to other platform would be not technically possible.	Set of electrical devices differs to nature of other participants in the project. Also for the reason of privacy protection it is not expected to use the data for further analysis.	For technical reasons there is no possibility with interoperability to other parts
LEPIDA	App for frail	Tabular data - frailty	Questionnaires evaluating frailty index of people, monitoring health condition and trends in time	Questionnaires and frailty index based on metrics could help future analysis of trends and patterns in health conditions	Analysis of frailty index
LHA BO	Involved in most of the tasks of other partners T1.1, T1.3-6	Tabular data - frailty	Questionnaires evaluating frailty index of people, monitoring health condition and trends in time	Questionnaires and frailty index based on metrics could help future analysis of trends and patterns in health conditions	Analysis of frailty index
ISRAA	GPS tracking	Time-series - location	GPS position for people. Those data are quite sensitive and it is not recommended to use them for any other future analysis	GPS position Falling accidents Heart-rate	Sleep patterns that will give warnings for possible Parkinson's disease.
SAM	Monitoring grid	Tabular data - frailty	Questionnaires evaluating frailty index of people, monitoring health condition and trends in time	Questionnaires and frailty index based on metrics could help future analysis of trends and patterns in health conditions	Analysis of frailty index
WAW	Participating in other tasks	Tabular data - frailty	Questionnaires evaluating frailty index of people, monitoring health condition and trends in time	Questionnaires and frailty index based on metrics could help future analysis of trends and patterns in health conditions	Analysis of frailty index

NIJZ	Participating in other tasks (T1.6)	Tabular data - frailty	Questionnaires evaluating frailty index of people, monitoring health condition and trends in time	Questionnaires and frailty index based on metrics could help future analysis of trends and patterns in health conditions	Analysis of frailty index

The main interoperability in respect to privacy and similarity of the data was identified in the following areas:

- LHA BO will analyze data obtained from questionnaires and frailty index with using monitoring grid.
- BUT in cooperation with hospitals FN Brno and FNOL use machine learning to analyse sleep patterns from time series obtained from watches for intelligent patients monitoring. Obtained data e.g. heart rate and ECG will be used for further data analysis. Data will be collected in data storage and with using monitoring grid (University - Austria) predictions of patient future state will be carried out.
- UHO cares for frail and monitor patients health conditions and their trends in time. The patient's data will be stored and analysed in monitoring grid. UHO will analyse pneumonia and frailty index.
- In LEPIDA – Italy uses questionnaire app for frail, which measures patient state during time interval. Data contains the frailty index and aim is to compute prediction the value in future. Collected data will be stored and frailty index analysed in monitoring grid.
- SAM is responsible for analysing and further processing of all data. Every member of project can obtain new predictions for its patient from this monitoring grid.

In order to comply with GDPR, all the data will be first strictly anonymised, including any information that could lead to the identification of a patient. All the predictions from the data will be targeted to overall trends to keep the privacy of the involved persons protected and highest priority.

Patient will be identified with “Unique Patient/Member ID” that will be saved in cloud service, which provides data encryption and also encrypted communication when data are shared using cloud. Uploaded data are owned by their creator and can be stored in cloud as long as needed. Data can be analyzed directly in cloud with machine learning algorithms or with other methods. Data can also be analyzed with external platform provided by project partners. Some medical devices and remote monitoring devices which are connected to the internet, can communicate with cloud service to store their data. Providers (healthcare centre, social care provider etc.) communicate with cloud service using FHIR (Fast Health Interoperability Resources).

Integration and Exchange of data in nice-Life project

Data will be exchanged between project partners using cloud service. In this part we will define medical data to exchange.

General description:

Exchange of medical data record in following detail:

- Outpatient reports, discharge reports
- Emergency card, patient summary
- Requests, examination results, RDG, PACS, descriptions

For simplification let's define basic dataset of data Exchange, based on PS (patient summary) standard, defined by European Commission.

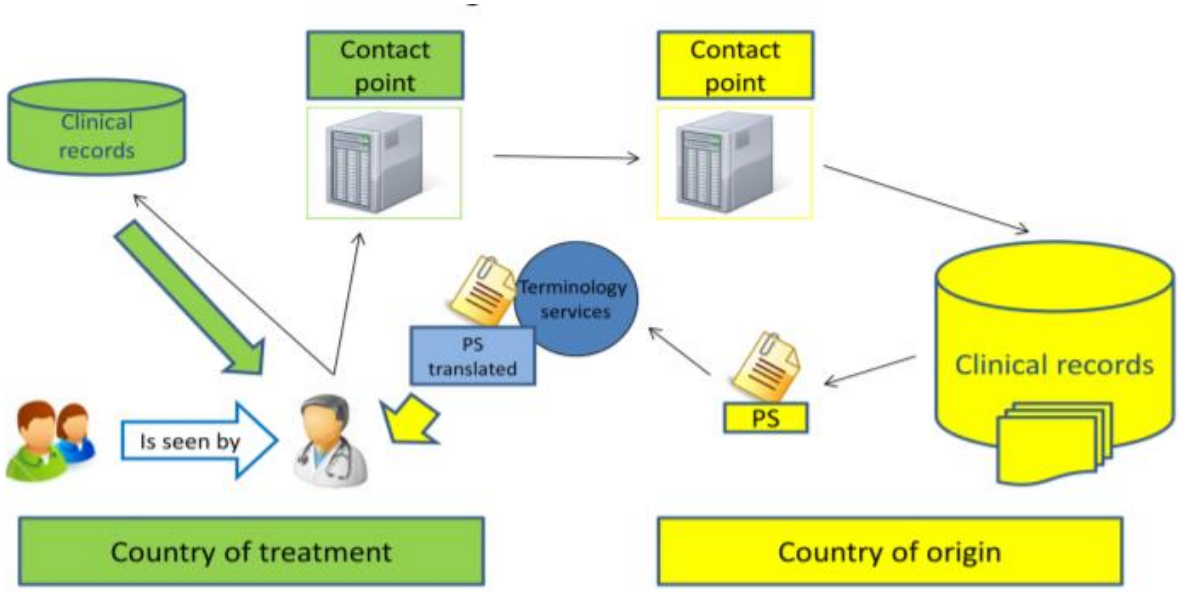
Definition of Patient Summary (PS)

Patient Summary provides information on important health related aspects such as allergies, current medication, previous illness, surgeries, etc. It is part of larger collection of health data called electronic Health Record. The digital Patient Summary is meant to provide doctors with essential information in their own language concerning the patient, when the patient comes from another EU country and there may be a linguistic barrier. On a longer term, not only the basic medical information of the Patient Summary, but the full Health Record should become available across the EU. The exchange of ePrescriptions and Patient Summaries is open to all the Member States.

Both ePrescriptions and Patient Summaries can be exchanged between EU countries thanks to the new eHealth Digital Service Infrastructure (eHDSI).

By 2021, both services will gradually be implemented in 22 EU countries: Austria, Belgium, Croatia, Cyprus, Czechia, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Slovenia, Spain and Sweden.

Patient Summary standard can be used for exchanging data as depicted below. All organizations connected to this cloud service can upload or download data when needed.



Patient Summary (PS) data set:

Patient Summary format consists of important items that can be used for data analysis. The content of data set is described below.

A. Patient identification and contact information

a) name, or names, surname of the patient,

b) birth number, if assigned,

c) number and type of electronically readable document proving identity,

d) date of birth,

e) sex, if specified,

f) citizenship,

g) the correspondence address of the patient, if it is not identical with the address according to letter

h) telephone number, e-mail address,

i) the language or languages in which the patient communicates,

j) the unique departmental identifier of the patient assigned to the patient by the Institute of Health Information and Statistics of the Czech Republic.

B. Identification and contact details of the registering provider in the field of general practice

a) business name or name of the registering provider, identification number of the person, if assigned,

b) telephone number, electronic mail address.

C. Identification and contact details of legal representatives or guardians or contact persons

a) name, or names, and surname of the person,

b) relationship to the patient,

c) telephone number, e-mail address.

D. Health Insurance Information

The code of the health insurance company and the number of the insured, if this number is not a birth number.

E. Urgent information

a) allergies:

1. verbal description,
2. a structured coded description, namely
   - 2.1. date of discovery,
   - 2.2. type of agent,
   - 2.3. type of agent,
   - 2.4. manifestation of an allergic reaction,
   - 2.5. degree of severity,

b) other risk factors:

1. verbal description,
2. a structured and coded description, namely
   - 2.1. date of discovery,
   - 2.2. type of risk factor,
   - 2.3. degree of severity.

F. General history

a) a verbal description containing information on:

1. the vaccinations carried out,
2. past health problems and diagnoses,
3. significant surgical procedures in relation to past health problems and diagnoses,

b) a structured coded description containing information on

1. Vaccination, namely

1.1. the name of the vaccine,

1.2. substance code,

1.3. date of vaccination,

2. Past health problems and diagnoses, namely

2.1. date or other time of origin,

2.2. date or other timing of termination,

2.3. health problem or diagnosis code,

3. performed significant surgical procedures, namely

3.1. performance code

3.2. execution date,

3.3. number of executions.

G. Current health problems and diagnoses and related data

a) current health problems and diagnoses:

1. date or other time determination of origin,
2. date or other timing of termination,
3. description of the health problem or diagnosis in free text,
4. code of the health problem or diagnosis,

b) significant surgical procedures in relation to current health problems and diagnoses:

1. description of the surgical procedure in free text,
2. performance code,
3. date of execution,
4. number of designs,

c) medical devices on which the patient's state of health depends or may depend:

1. verbal description,
2. date of implantation or start of use,
3. code of the medical device,

d) treatment recommendations that do not include drug treatment, date of enrollment, free text recommendations,

e) a verbal description of the patient's self-sufficiency or disability, date of origin and code.

H. Medications used

a) name and code of the drug,

b) strength, form, method of administration, by code,

c) quantity / dose, dosage,

d) the beginning and time of administration or the date of termination of administration.

I. Lifestyle factors

a) verbal description of the factor,

b) factor code,

c) the date or other temporal action of determining the beginning of the action of the factor,

d) quantity or unit of measurement.

J. Pregnancy

Code of the method of determining pregnancy and the expected date of delivery.

K. Physical finding

a) systolic and diastolic blood pressure, heart rate and date of their measurement,

b) height and weight, namely value, unit and date of measurement.

L. Diagnostic tests

Blood type and Rh factor by text and code, date of determination.

M. Accompanying data

a) date of creation of the patient summary,

b) the date of the last update of the patient summary,

c) identification data of the provider who created the patient summary, namely business name or name, address of the registered office or address of the place of business, identification number of the person, if assigned, or other identifiers of the provider,

d) the name (s) and surname (s) of the doctor who drew up the patient summary; this item is not reported in the case of a patient summary supplemented continuously by more physicians or resulting from the aggregation of data.