RES-Q
Data for Life

Data Protection Impact Assessment for Registry of Stroke Care Quality (RES-Q)

IRENE
Network for stroke care improvement

cost
EUROPEAN COOPERATION IN SCIENCE AND TECHNOLOGY

COST is supported by the Framework Programme Horizon 2020

Document control:

	Name and role	Contact details
Document Completed by	Ing. Václav Pasáček, RES-Q Senior Developer Miroslav Vařecha, Ph.D., RES-Q Data Scientist	vaclav.pasacek@fnusa.cz miroslav.varecha@fnusa.cz
Data Protection Officer name	Mgr. et Mgr. Zuzana Ondrůjová	zuzana.ondrujova@fnusa.cz
Document approved by (this should not be the same person that completes the form)	Prof. Robert Mikulík, MD, PhD RES-Q Founder	robert.mikulik@fnusa.cz
RES-Q Global – partner non-governmental organization (NGO)	Ing. MgA. Veronika Svobodová (Director), Prof. Robert Mikulík (Management Board), doc. Tomáš Pitner (Management Board), Dr. Václav Stupka (Management Board)	svobodova.stroke@gmail.com mikulik@hotmail.com pitner@muni.cz stupka@fi.muni.cz
Organization co-financed by State budget, directly controlled by Ministry of Health of the Czech Republic; list of such organizations can be found here: https://www.mzcr.cz/organizace-v-prime-pusobnosti-ministerstva-zdravotnictvi/ Legal Person Identification Number: 00159816	St. Anne's University Hospital in Brno ("FNUSA"), International Clinical Research Centre ("ICRC") – integral part of the hospital)	

Date Completed	Version	Summary of changes
13 December 2021	V1.0	First draft
4 January 2021	V2.0	Revision
13 January 2021	V3.0	Final version

Screening questions

Please complete the following checklist:

	Section	Yes or No	N/A	Comments
1	Does your project involve any automated decision making, evaluation or scoring including profiling and predicting using information about a person? Does the outcome from your project decide who gets access to services?	No		
2	Does your project involve any sensitive information or information of a highly personal nature?	Yes		RES-Q collects patients' level data related to stroke care quality. Such data include age, gender, stroke date, vascular risk factors in patient's history, type of stroke, type of stroke diagnostic, treatment and outcome. RES-Q does not collect any identifiers. Another type of data which RES-Q collects is user information while registering on the RES-Q platform. During online registration as a user, they accept terms and conditions for participation. RES-Q collects only necessary credentials to recognize and contact users: title, name, phone number, e-mail address, country, select hospital name. Users will be validated by the local coordinator of their hospital.
3	Does the proposal involve any data concerning vulnerable individuals who may be unable to easily consent or oppose the processing or exercise their rights?	Yes		Some patients with stroke can be considered vulnerable individuals. This group may include children, unconscious or mentally ill persons, usually the elderly patients and cases where there is an imbalance in the relationship between the position of the individual and the controller. Acute stroke can hit people of any age, but is predominant in the elderly. One of the very common issues associated with acute stroke is speech impairment and therefore most information can be then provided by caregivers or from the national or hospital healthcare system.

4	Does your project involve any innovative use or applying new technological or organizational solutions? This could include biometric or genetic data, the tracking of individuals' location or behavior?	No		
5	Does your project match data or combine datasets from different sources?	Yes		Currently we combine RES-Q preprocessed data with RES-Q-formatted data from some national registries, e.g. from Thailand national registry. As a part of an ongoing grant project we will also match RES-Q dataset with a dataset from Institute of Health Information and Statistics of the Czech Republic (ÚZIS). The Institute is an organizational unit of the state and has been established by the Ministry of Health of the Czech Republic.
6	Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	Yes		Information is gathered from hospitals' electronic health records. We present patient information flyers with details how and why data is used and what security measures are taken to ensure its security. A privacy notice will be available on the RES-Q webpage.
7	Does your project process data that might endanger the individual's physical health or safety in the event of a security breach?	No		
8	Is this a new project or have the requirements for your project changed since its initiation? Are you sharing new information or linking to new datasets that were not part of the original project specification? Have you added any new streams to your project?	No		This project started in 2016 before GDPR was adopted. This project was approved by the former hospital director, MUDr. (MD) Martin Pavlík, Ph.D., EDIC, DESA. The Ministry of Health of the Czech Republic was also informed by letter. In 2018 the GDPR brought significant changes in European legislation – the compliance audit was realized in place. New legal requirements will be met through this DPIA. The project itself has not changed in the main idea, but the register of data could serve as a data source not only for primary purpose (improving the quality of health care), but also for secondary purpose (specific healthcare research goals). In case of linking in the future, we will update this DPIA.

Data Protection Impact Assessment

This Data Protection Impact Assessment (DPIA) aims to ensure that the project is compliant with GDPR and Czech data protection legislation as well as European Data Protection Board (EDPB) Guidelines. This document will be updated if further European Data Protection Board (EDPB) or Czech supervisory authority – The Office for Personal Data Protection (Úřad pro ochranu osobních údajů, "ÚOOÚ") – guidance is published or there is change in legislation. Methodologies of other European countries' supervisory authority were reviewed and for the purpose of this document the methodology of the Information Commissioner's Office (ICO) in the UK was also used.

This DPIA is the basis of a "privacy by design" approach, to help meet privacy and data protection expectations of FNUSA patients and employees, partner hospitals and organizations, its patients and employees, researchers and other stakeholders. It is intended to be prospective and proactive and should act as an early warning system by considering privacy and compliance risks in the initial design and throughout the project.

Purpose and benefits

- Identifying and minimizing the privacy risks associated with this project.
- Carry out an assessment of the impact of the envisaged processing operations on the protection of personal data due to legal precaution, even though the RES-Q project was started before 2018 (obligatory DPIA wasn´t stipulated by law until 2018 in the Czech Republic).
- Coordinate with people within the organization, with partner organizations and with the people affected to identify and reduce privacy risks.
- Determine the appropriate controls needed to protect personal data i.e. technical, procedural and physical.
- Ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Help produce better policies and systems and minimize the risks, thus improving the relationship between organizations and individuals (in this case, increase credibility of RES-Q and the hospital from the patient's point of view).
- The Office for Personal Data Protection may ask an organization whether they have carried out a DPIA. It is often the most effective way to demonstrate to the Office for Personal Data Protection how personal data processing complies with Data Protection legislation.
- External lawyers and IT experts recommended to carry out the DPIA prior to realizing any other action including the new contracts with the partner hospitals. The same recommendation was given by the FNUSA DPO.

Supplementary guidance

- The Office for Personal Data Protection, Czech Republic DPIA guidelines
- The Office for Personal Data Protection, Czech Republic conducting privacy impact assessments code of practice
- EDPB Guidelines on Data Protection Impact Assessment
- ICO's Data Protection Impact Assessment under GDPR guidance
- Foreign states' good practice could be helpful for RES-Q as the Czech Republic doesn't have any specific guidelines for data processing in research. Therefore, we use United Kingdom supervisory authority guidance and UK guidance on governmental level is very useful for Czech practice as well:
- The ICO's Anonymisation: managing data protection risk code of practice may help organizations to identify privacy risks associated with the use of anonymised personal data.
- The ICO's Data sharing code of practice may help organizations to identify privacy risks

associated with sharing personal data with other organizations.

- The ICO's codes of practice on privacy notices, as well as other more specific guidance, will also help an organization to focus DPIAs on those issues.
- The Government Data Programme has developed a Data Science Ethical Framework to help organizations understand the benefits and risks of using personal data when developing policy. The Framework can be used as part of the process to help you describe information flows and identify privacy risks and solutions.

DPIA methodology and project information

The RES-Q registry was launched in cooperation with the European Stroke Organisation in 2016 with the aim to provide a platform for hospitals to monitor their stroke care quality. Since its start, hospitals from 75 countries have joined the RES-Q registry. RES-Q now provides feedback in a form of presentation of statistical metrics describing stroke care quality, spreadsheet with same statistics and raw data downloadable by hospitals for their own analysis. RES-Q is going to become a non-governmental organization, titled RES-Q Global, with the purpose to ensure technical and further development of the registry and data administration, while the FNUSA-ICRC Stroke Program will use the data for scientific purposes.

Aim

The primary aim of RES-Q is to improve the quality of stroke care worldwide. Data structure follows the stroke patient pathway. RES-Q provides hospitals/healthcare services with the information and tools they need for quality improvement and service development to ensure that patient care and experience is of the highest possible standard. To achieve such a goal, quality data are collected, analyzed, presented to users, and published in summary format. Data is also available to users in source data format. Rights to access source data format are defined and described on the RES-Q website.

Data collected in RES-Q can be used also for a secondary purpose – research related to stroke issues and stroke care [processing based on Art. 6 (1) (e) processing necessary for the performance of a task carried out in the public interest in connection with the exception from prohibition of processing special categories of the data (health data) under Art. 9 (2) (j) processing necessary for the purposes in the public interest, scientific research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law (Czech law – § 16 of Data Processing Act Nr. 110/2019 Coll.) which is proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject]. Data structure allows users to answer questions on association e.g. between quality of stroke services and outcome, patients history/type of diagnostic/type of treatment and outcome.

RES-Q description

Registry of Stroke Care Quality RES-Q is a platform for quality improvement in healthcare. It consists of a registry and built in functionalities to facilitate quality improvement especially through feedback mechanism. The RES-Q registry is until the beginning of 2022 governed by the FNUSA and runs on FNUSA's infrastructure. In 2022 RES-Q registry governance will transfer to RES-Q Global NGO which will use professional and secure production-grade infrastructure with healthcare certifications (e.g. OVHcloud). Reason for transfer is better access to hosting and services with improved cyber security. There will be less downtimes, faster hardware and existence of backup in different geo-location.

RES-Q was originally developed in cooperation with and under the umbrella of the European Stroke Organisation to improve quality of in-hospital stroke services but is expanding also to improve healthcare in the outpatients setting and in life after stroke (e.g. rehabilitation). Nowadays RES-Q consists of three parts, each related to different stages of the patient care pathway: pre-hospital, hospital and post-hospital care. Majority of data is captured at patient level but some data (e.g. pre-hospital care) is captured as summary statistics.

Pre-hospital care (Emergency Medical Service)

Organizations which provide Emergency Medical Service (EMS) are internally structured into branches (typically geographically). RES-Q collects aggregated data for all stroke-related patients treated by a single branch in a certain time period. On a branch level RES-Q also visualizes collected metrics over time and provides data for EMS Angels Awards evaluation (granted by ANGELS Initiative – a non promotional health care initiative).

Hospital care (Acute and post-acute care)

RES-Q collects patient data from participating stroke centers via web-based form. There are multiple data collection forms (differs in level of detail and main subdomain) in several languages. All forms are oriented to collect data which could be used to calculate care quality and performance metrics like time of stroke onset, admission, treatment, imaging, details of treatment and further care. On stroke center level RES-Q also visualizes near real-time calculated care quality and performance metrics. Ones per quarter or year provide offline in-depth reports of care quality and provide data for European Stroke Organization Angels Awards / World Stroke Organization Angels Awards evaluation. Optionally patients can be identified by Person ID and country for linkage with data from other sources like Institute of Health Information and Statistics of the Czech Republic (UZIS).

Post-hospital care (Post-discharge quality of life)

Patients who were discharged from hospital after a stroke (or their caregivers) will use mobile applications to report their quality of life and different problems related to life after stroke like spasticity, depression, quality of life and other selected conditions. This application can alert a user that there is a potential problem which should be treated by an appropriate specialist. Optionally patients can be identified by Person ID and country for linkage with data from acute and post-acute care in RES-Q.

RES-Q Infrastructure

Nowadays RES-Q is operated by FNUSA on it's internal infrastructure. Such a deployment has a set of limitations (required proxy usage, forced network policies, etc.) and potential risks (cyber-attack on FNUSA can affect RES-Q, shared cloud cluster with other projects, etc.). In the near future RES-Q will be operated by RES-Q Global NGO based on a legal agreement between FNUSA and RES-Q Global.

Data processing

For improving quality of stroke care – primary purpose

Data is currently collected for local sites which will enter data for appropriate patients via web-based form or mobile application (in future). Patient identifiable data is only visible to individual sites. Practices from local sites can access their own data (only) and use it for quality improvement (QI) purposes based on Art. 6 (1) (f) GDPR – processing necessary for the purposes of the legitimate interests pursued by the hospital as a controller and a third party (patients concerned), where such interests is supposed to overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (data subject could be a child in theory, but very rarely) – so called "test of balance between aim pursued and data subjects fundamental rights" in connection with Art. 9 (2) (i) processing necessary for reasons of public interest in the area of public health, such as ensuring high standards of quality and safety of health care. No other organization or individual will be able to access these identifiable data. Once the data have been pseudonymised (by giving a new ID code to each patient on local sites), national coordinator or other responsible person can ask for data analysis. RES-Q operates in an 'encrypted/electronic only' data transfer policy for all patient level data using HTTPS and stores data on secure endpoints. Use of portable storage media and email is prohibited. Data processing assets are operated in secure locations.

For research – secondary purpose

Data stored in RES-Q for primary purposes can be used also for research purposes as specified above. For future prospective scientific projects, Study Protocol, Informed Consent, Information for the patients and other necessary documentation will be submitted to the Ethical Committee and go through institutions approval procedure, which are in place. Current data can be used for projects focused on ensuring high standards of quality and safety of health care, but could be qualified as research studies (improving care and medical research is often closely connected) and the RES-Q team will conduct export and pseudonymization of data upon request and approval by National coordinator/s. Exported data is then sent to the research team that requested it as a simple attachment in an email message.

Aggregated data

Aggregated data are not the subject of GDPR compliance rules. RES-Q users can freely share their aggregated data for quality improvement and research (open data).

Data transfer

Despite the fact that users already provide pseudonymous data to RES-Q they must ensure that data collection is in line with all legal requirements including rules for data retention period in their countries. This is the part of a renewed contract with users to be signed within 2022 and onwards.

Raw data download

Users can download raw pseudonymised data from their stroke center.

Third party applications for data

Only pseudonymised patient data from acute and post-acute care, Emergency Medical Service and life after stroke parts can be shared.

All mentioned types of data are accessed by St. Anne's University Hospital in Brno and RES-Q Global, NGO for both research purposes and for improving stroke care quality.

All other applications for data have to specify purpose and required time periods and countries. National coordinators of those countries decide if data of their country will be shared for this specific purpose.

Retention of data

In line with the Guidance document (Věstník) from the Ministry of Health of the Czech Republic (https://www.mzcr.cz/vestnik/vestnik-c-10-2021/), is RES-Q recommended to use for stroke care quality monitoring in the Czech Republic. To fulfill this role RES-Q will monitor quality improvement in longer time periods and also be able to provide data for future research projects, RES-Q will keep data securely for at least a minimum period of 10 years. Czech legislation doesn't specify any maximum retention period. Country specific requirements for retention of data will be reflected based on contracts with users and national coordinators.

DPIA Consultation

The RES-Q team consulted the problems of data processing with many relevant people (both internal and external stakeholders) while conducting this assessment, consultation is an important part of a DPIA and allows people to highlight privacy risks and solutions based on their own area of interest or expertise. Consultation can take place at any point in the DPIA process and may include the project management team, Data Protection Officer, designers, IT specialists, lawyers, researchers, analysts, statisticians and senior management of the institution.

Data Protection Officer FNUSA, lawyers FNUSA, lawyers and IT specialists from Masaryk University, Brno, Czech Republic. Consulting data subjects would be disproportionate and have little sense in the context of this registry which has been existing for more than 5 years.

The data flows and charts have been consulted with experts from the Technical Faculty of IT and Design, Aalborg University, Denmark, who have been contributing to the RES-Q development since 2020.

Publishing DPIA report

Publishing a DPIA report is not a legal requirement and it will not be publicly available, but its existence will be noted on our webpage. We will make this DPIA available to all RES-Q registered users to read and download.

Data Information Flows

Currently RES-Q consists of three parts, each related to a one stage of the patient care pathway. Data flow in each stage of the patient care pathway will be described separately.

Pre-hospital care
Data is aggregated on the side of EMS organization/branch therefore RES-Q handles only data de-identified by aggregation.
Anonymized by aggregation at source.

Data types

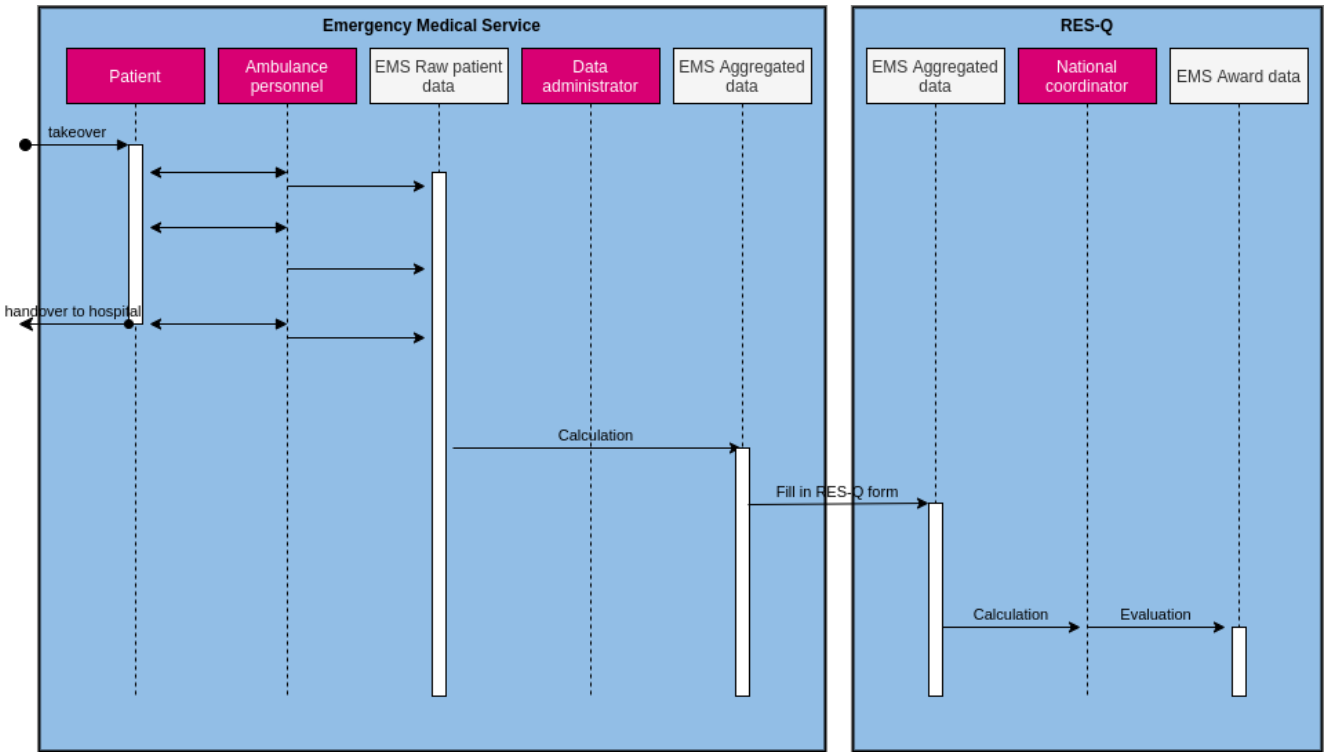
- **EMS Patient raw data** – medical data related to specific patients: name, ID, age, gender, time of arrival, symptoms, etc.
- **EMS Aggregated data** – for all patients with stroke symptoms in the same branch, at the end of each quarter calculates key metrics like average time on scene, percentage of prenotification to hospital, percentage of patients with known medication details. Such data are de-identified by aggregation.
- **EMS Award data** – Information that EMS branches receive Gold, Platinum or Diamond EMS Angels Awards. This data will be publicly available on the RES-Q website.

Data flow subjects

- **Patient** – person with stroke symptoms which has been transported by Emergency Medical Service to the hospital
- **EMS organization branch** – part of organization which provides emergency transport of patients into medical facilities. It also collects *EMS Patient raw data*.
- **RES-Q** – stroke care quality registry, as an administrator, it has direct access to EMS Aggregated and EMS Award data

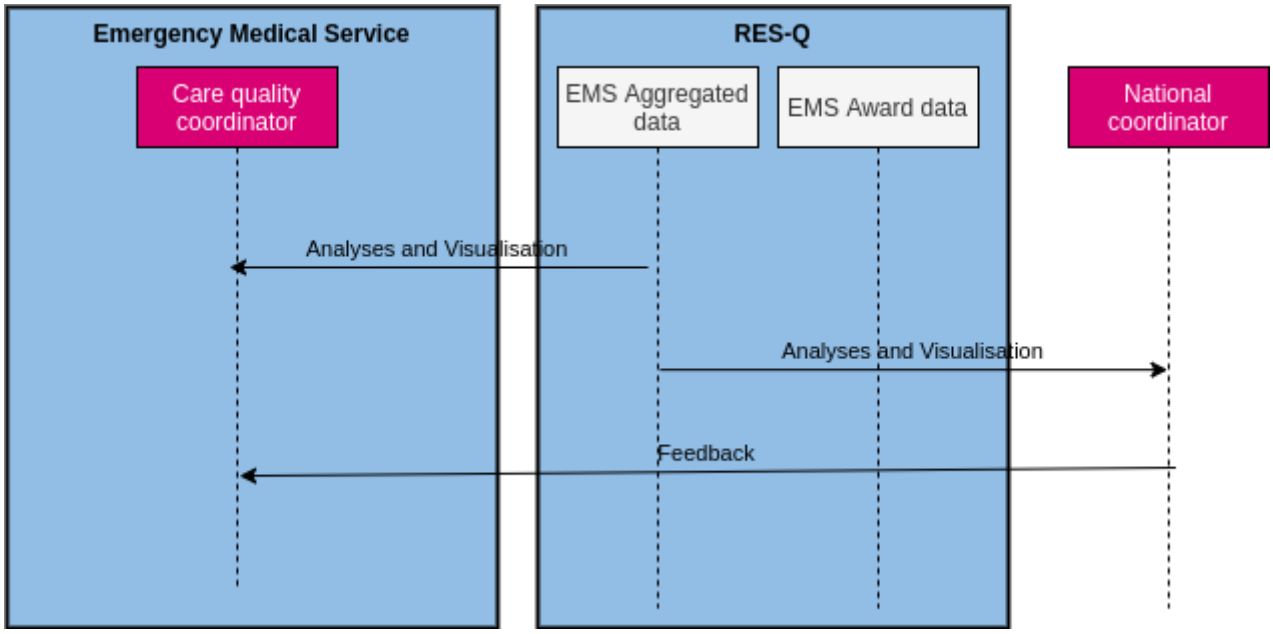
- **EMS Data administrator** – RES-Q user designated by EMS organization which calculates EMS Aggregated data.
- **EMS National coordinator** – user which quarterly approve European Stroke Organisation (ESO) / World Stroke Organization (WSO) EMS Angels Awards

EMS organization branch during its operation collects *EMS Patient raw data*. At the end of each quarter branch calculates *EMS aggregated data* and inserts them in RES-Q via web-based form. Therefore RES-Q handles only data which are already anonymized by aggregation on it's source.
Based on *EMS Aggregated data* RES-Q based on the set KPI criteria, calculates levels of EMS Angles Awards for all branches who enter data in this period. Then National Coordinators evaluate and approve or reject the level of award.



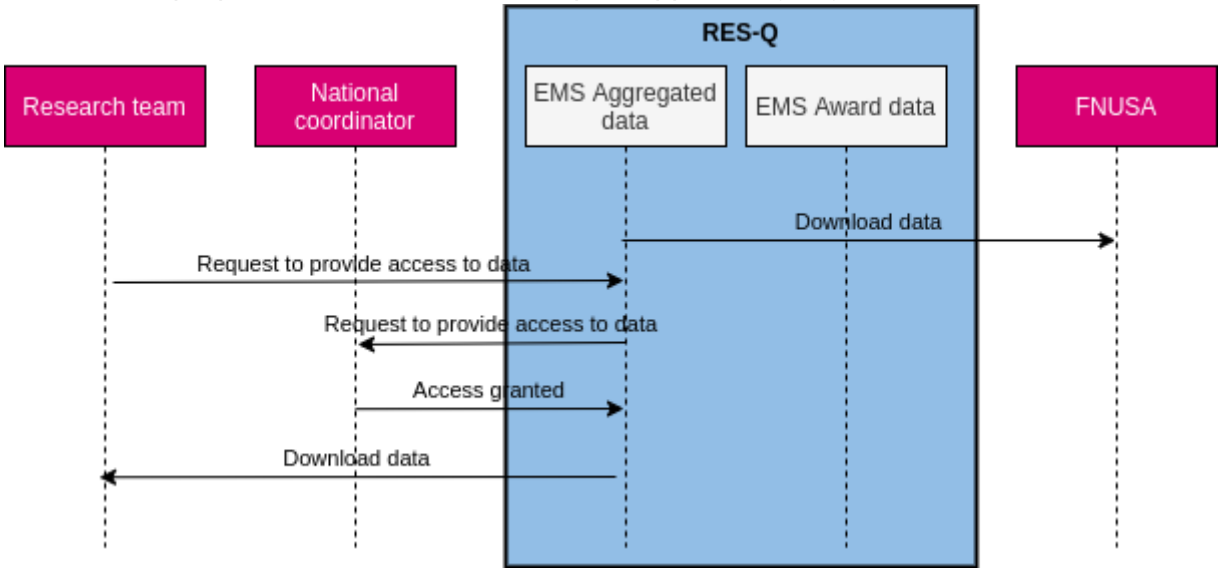
Data collection in Emergency Medical Service

For the purpose of care quality improvement each EMS organization branch has access only to its own data. National coordinator has access to data from all EMS branches operating in his country.



Data usage in care quality improvement

If a third party wants to use RES-Q data for research purposes, they have to seek an approval from the country's National Coordinator and sign a Data Sharing Agreement. Data is also shared with FNUSA for research purposes, without a need of explicit approval by any National coordinator.



Data usage in research

Hospital care

RES-Q optionally allows to collect a pseudonymized patient personal identifier to link data with other sources. It's only possible if the patient signs up the informed consent, typically as part of research projects.

Patient identifiable data from acute and post-acute care is only visible to individual stroke centers and to RES-Q Global (non-governmental organization), if required for administrative purposes. Please note, RES-Q Global only access the data on very rare occasions, examples of which are listed below:

- System 'debugging' investigations, if problems are experienced with processes where patient identifiable data is involved. Examples might include duplicate checks, re-admission processing, and validation processing. Note, wherever possible, system tests are undertaken on test systems using dummy/fake patient identifiable data. However, processing of live data may have to be examined in detail in rare but limited circumstances.
- Data linkage exercises to validate linkage success – this is usually limited spot checks. Bulk

access to patient identifiable data is necessary to undertake linkage exercises.

No other organization or individual will be able to access *Patient raw data*.

Data types

- **Hospital data –** all kinds of information which are gathered by a hospital in Electronic Healthcare Records including names, personal ids, admission and discharge reports, all CT, MR and laboratory results.
  Note: RES-Q platform doesn't operate with this data type at all.
- **Patient raw data** – medical data related to individual patients such as age, gender, time of admission, patient ID, imaging, stroke type, treatment.
  Pseudonymized personal identifier.
- **Preprocessed patient data** – Raw data without a personal identifier.
- **De-identified patient data** – Preprocessed patient data with the following de-identification changes
  - All dates and times (admission, imaging, treatment, discharge, etc.) are substituted with calculated durations (hospital stay, Door-to-needle time, Door-to-groin time, etc.) and quarter of admission
  - Removed patient label and hospital name
  - Hospital ID is substituted with random number (due to specific requirements, this does not apply to the Czech Republic)
- **Aggregated data** – statistical data calculated for all patients in a certain time period (quarterly, annually, bi-annually) in a single hospital or country e.g. patient median age, median Door-to-needle time, median Door-to-groin time, recanalization patient rate. Aggregated data are not personal data for a purpose of data protection law as GDPR.
- **Evaluation results** – for facilities which fulfill all required criteria, there are three different levels of awards – Gold, Platinum and Diamond ESO/WSO Angels Awards. This data will be publicly available on the RES-Q website.

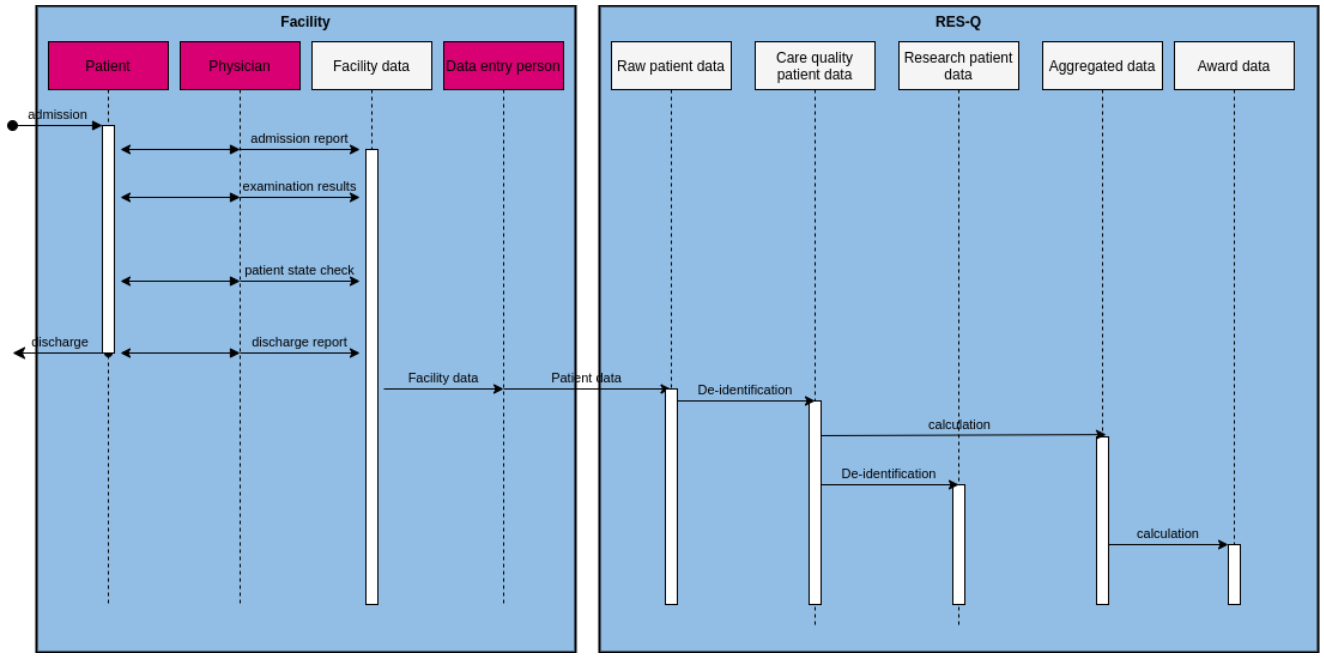
Data flow subjects

- **RES-Q Admin** – Person entrusted by RES-Q Global to administer and maintain the RES-Q platform
- **Hospital** – Users registered as employees of certain hospitals which are responsible for patient data collection (aka. data entry person)
- **National coordinator** – users with specific privileges on top of standard user privileges:
  - quarterly approve ESO/WSO Angles Award program for stroke centers
  - Access to preprocessed patient data and aggregated data for all stroke centers in their country registered in RES-Q
  - Approvers for sharing national data with third party through Data sharing agreement
- **FNUSA** – St. Anne University Hospital is primary research partner of RES-Q
- **Third party** – any organization which doesn't have access to De-identified or Aggregated data can send a request to get access to data to RES-Q. Such a request has to contain purpose, data source countries and time interval. It will be evaluated by national coordinators of affected countries. Nothing is shared without national coordinator approval.
- **Public** – data available publicly on RES-Q website without user login

	RES-Q Global (admin)	Hospital (user/data entry entity)	National coordinator	FNUSA (user for research)	Third party	Public
Patient raw data	yes	yes	No	No	No	No
Preprocessed patient data	yes	No	No	No	No	No
De-identified patient data	yes	Own hospital data only	Own country data only	Yes	Approval required	No
Aggregated data	yes	Own hospital data only	Own country data only	Yes	Approval required	No
Evaluation results	yes	yes	yes	yes	yes	yes

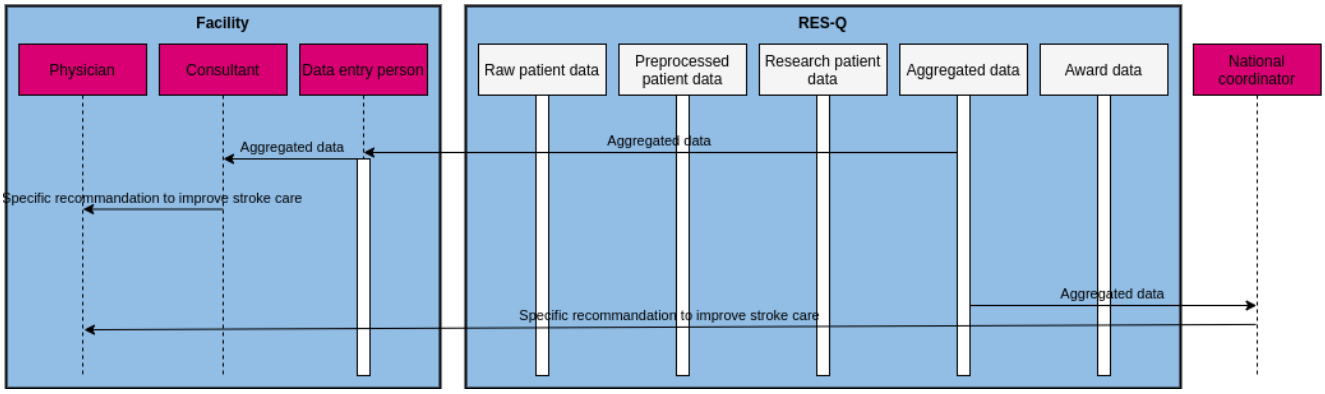
Accessibility of data for different types of users

Stroke centers collect *Hospital data* in their EHR systems. Based on these data entry persons then (typically after patient discharge) fill in RES-Q form. This process creates Raw patient data in the RES-Q system. Additional processes which transform Raw patient data into Preprocessed patient data, De-identified patient data and Aggregated data are started periodically.



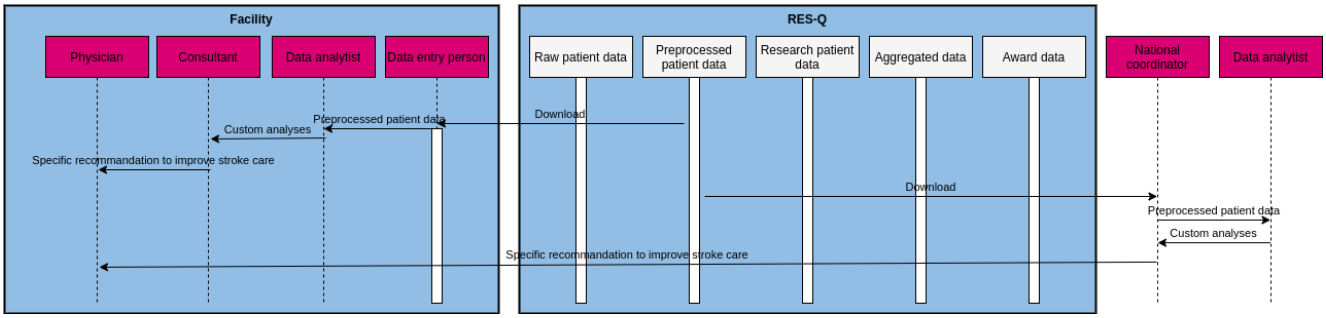
Data collection basic workflow

Primary data usage of data collected, processed and aggregated by RES-Q is care quality improvement. It directly visualizes aggregated data as online dashboards and offline detailed reports. Such analyses provide the quality metrics on which bases care quality management could be handled.

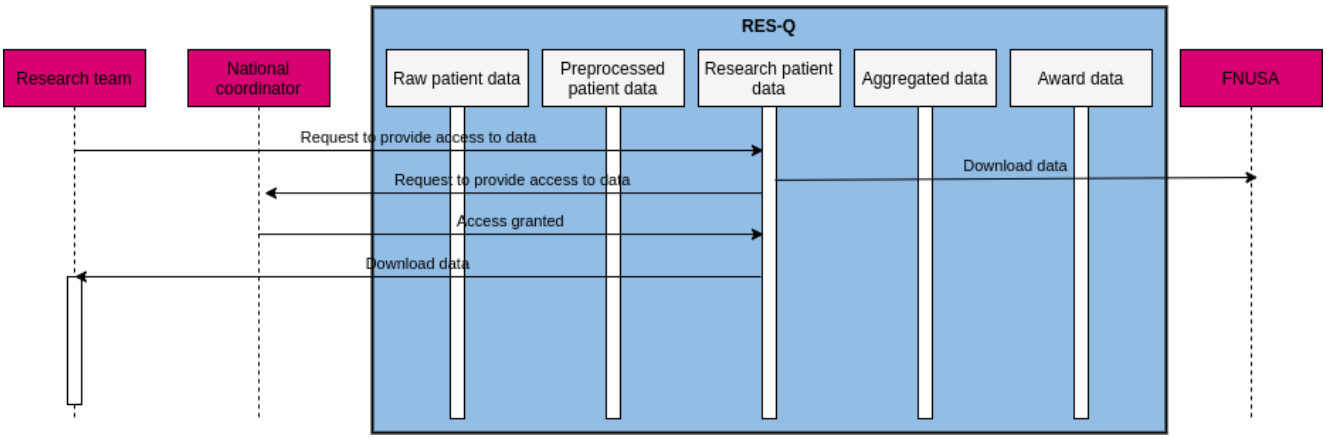


Care quality improvement with RES-Q analyses workflow

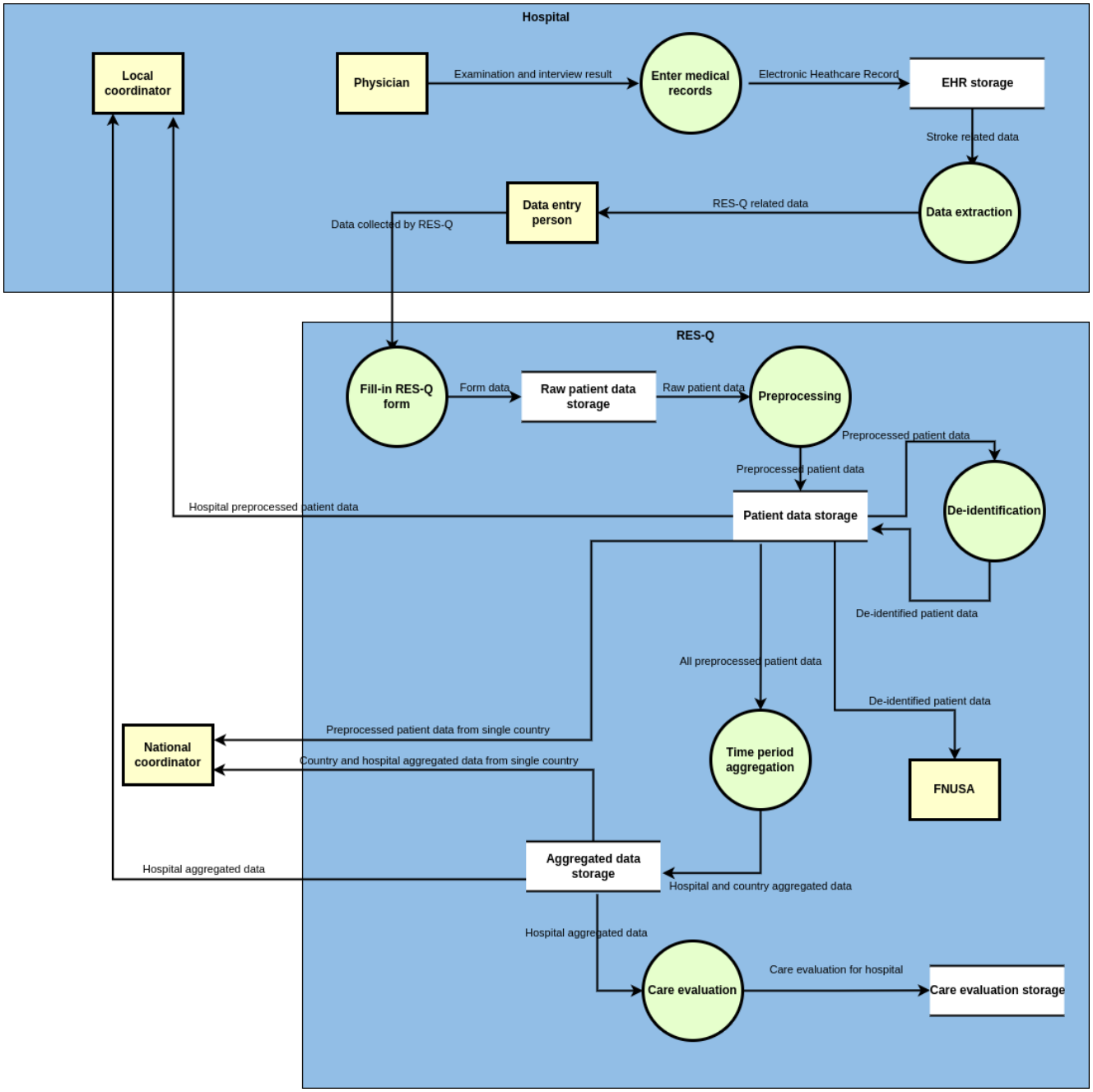
In very specific cases where the analyses provided by RES-Q doesn't fulfill all user needs, it's possible to download *Preprocessed Patient data* and do a custom data analyses by the hospital itself or by national coordinator.



Care quality improvement with self-made analyses workflow



Data workflow for research purpose



Data flow diagram of hospital care related with RES-Q

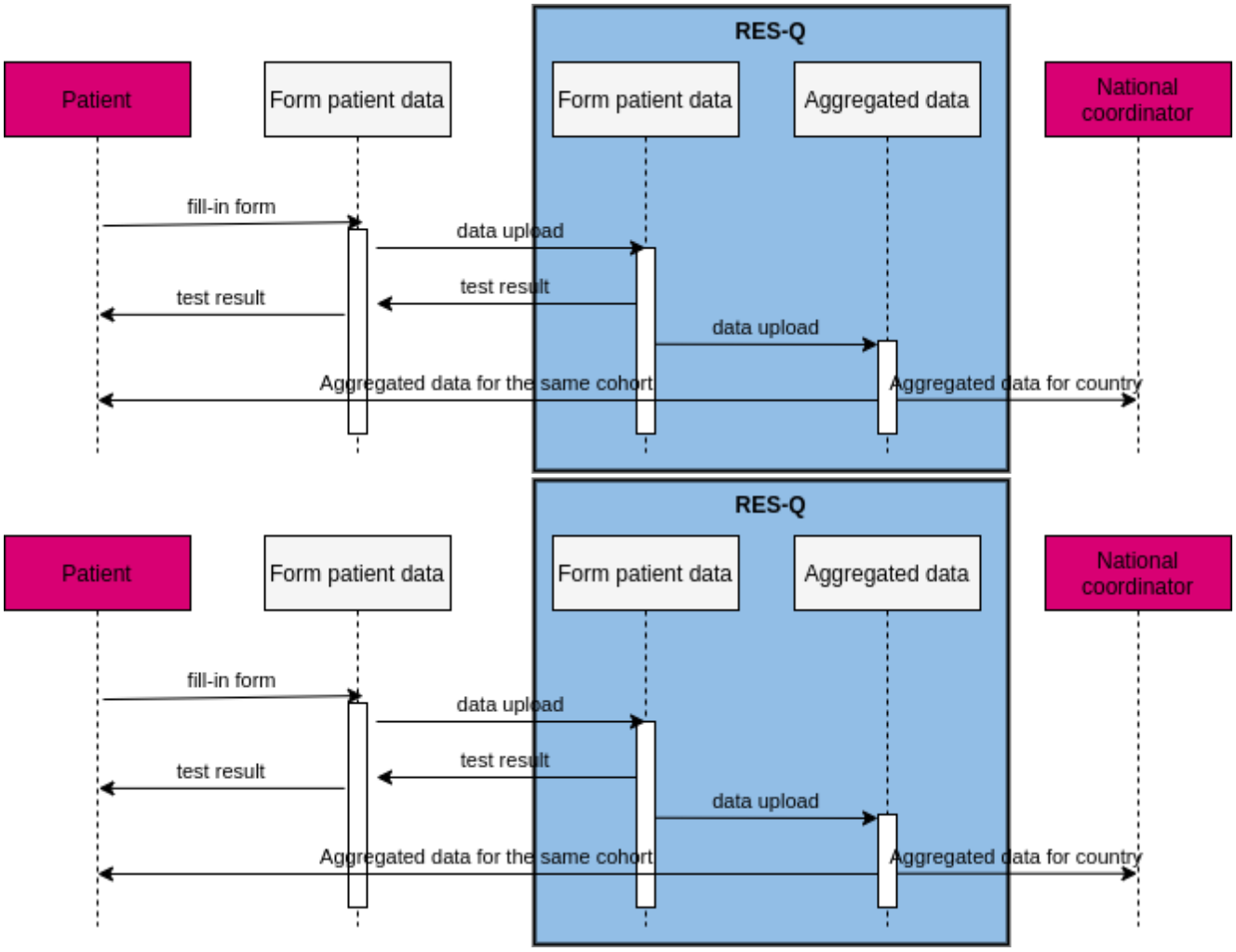
Post-hospital care (PH)

Data types

- **PH Patient raw data** – personal identifier of patient and patients answers to multiple RES-Q form questions including ability to walk, spasticity, actual mood, etc.
- **PH Aggregated data** – statistical data calculated for all patients discharged after stroke in different delays (e.g. 3 months after, after 1 year, etc.). Typically mRS distribution, quality of life indicators, depression level.

Data flow subjects

- **Patient** – person discharged from hospital after stroke, which use RES-Q mobile app to monitor quality of life after stroke (= data subject)
- **National coordinator** – Person responsible for care quality management within a country



RES-Q web-tool users

Web-tool users (those who enter and sign-off the data) register themselves (legal basis = consent) on the RES-Q web-tool. Details (including name, title, email address, place of work and contact number) are kept in the RES-Q and are accessible to the RES-Q team for creating user accounts to allow access to the RES-Q platform and for administrative purposes (communication activities, reporting etc.).

RES-Q mobile phone app users

New mobile application allowing entering patients data into RES-Q from phones and tablets is developed. It will allow user registration, data entry and progress/statistics information of the user's hospital records status. It might also notify users when certain conditions and deadlines are approaching.

Outcome mobile phone app users

We obtained a grant for development and deployment of an outcome mobile application allowing monitoring of quality of life and health conditions of stroke patients released from hospital after their stroke in Czechia. This application will allow patients and/or their caregivers to log into the application and conduct self-administered surveys evaluating physical and mental health of stroke victims at 3, 6, 12 months after the discharge. Patients will log using their national health insurance ID. Which will be stored also in the RES-Q database and it will allow for linking of Outcome application results with RES-Q patient records. These selected patients will sign informed consent.

Transferring personal data outside the European Economic Area (EEA)

Transferring personal data outside the European Economic Area follows the same principle as the transfer of personal data inside EEA. These principles are compliant with the GDPR and ensure the highest level of data protection. Data collected in countries within EEA are not transferred to countries outside the EEA. Principles of data transfers outside of the EEA are the same as inside the EEA. As users can access only their own preprocessed patients data, therefore it's not necessary to assess appropriate safeguards (under GDPR, Article 46).
Contracts with the national coordinators cover responsibilities and authorization to share the data.

Justification for collecting personal data

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. It may not be necessary to process certain data items to achieve the purpose. They may be irrelevant or excessive leading to risk of non-compliance with the GDPR and Czech national legislation – Personal Data Processing Act (No. 110/2019 Coll.).

The extent of data collected in RES-Q is decided by professional societies according to the medical guidelines. Extent reflects the needs of quality improvement in stroke. For secondary research use of data the extent can be broader but follows the research protocol and comply with the specific approval for research projects (e.g. ethical committee, DPO, etc.). In prospective research studies there is typically also a need for informed consent.
The tables below list and justify personal data items needed to achieve the lawful aim of a project specified above that requires information on individuals and their personal characteristics. There are two sections in the table below, one for personal data and one for personal sensitive data items. We have two tables, one for patients' records and another for RES-Q registered users.

RES-Q registered users:

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Personal Data			
Name	Yes		We require the name of the RES-Q user to validate his/her activity in the selected home hospital with the local coordinator. We also use names in communication with users and for creating login names to RES-Q.
Email Address	Yes		We require user to provide working email address so system can send him login credentials after registration and for password reset
Hospital Name	Yes		We require the user to provide the country name and hospital name he works in, so we can assign his user account to access this hospital data.
Home Phone Number	Yes		In case we need to urgently contact the user and we cannot reach the user by email, we also ask them to provide their phone number.
Online Identifier e.g. IP Address/Event Logs	Yes		Collected for users of the due to the make-up of the RES-Q web-tool (how the equipment needs to work with the internet) but this information is not accessed or used in any way.
Website Cookies	Yes		We use technical cookies to monitor usage of our services.

Mobile Phone / Device No		N/A	
Device Mobile Phone / Device IMEI No		N/A	
Location Data (Travel / GPS / GSM Data)		N/A	
Device MAC Address (Wireless Network Interface)		N/A	
Sensitive Personal Data			
Physical / Mental Health or Condition		N/A	

Patients:

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Personal Data			
Name		N/A	
National health insurance ID	Yes		For a limited number of patients (so far planned only in Czechia) we also collect the National health insurance ID in a hashed (one-way encrypted) form. This identifier will allow us to link survey data from Outcome mobile app to RES-Q patient's records and to the Institute of Health Information and Statistics of the Czech Republic. These selected patients will sign an informed consent.
Address		N/A	
Postcode		N/A	
Date of birth		N/A	
Date of death (discharge)	Yes		We collect the date of admission of patients into the hospital and the date of discharge from the hospital. In case the patient died in the hospital, then the discharge date is the same as the date of death.
Age	Yes		Elderly age is the most important risk factor for suffering a stroke.
Sex	Yes		All collection forms include sex field. Primary reason for this information is medical. Women suffer strokes usually at higher age with more severe consequences. It might also allow us to study if the quality of care is the same for men and women in all hospitals/countries.

Living Habits	Yes		Information on smoking, risk factors, treatments before stroke.
Email Address		N/A	
General Identifier e.g. Hospital Name	Yes		Patient's record contains a unique label/ID, hospital name and hospital ID.
Home Phone Number		N/A	
Online Identifier e.g. IP Address/Event Logs		N/A	
Website Cookies		N/A	
Mobile Phone / Device No		N/A	
Device Mobile Phone / Device IMEI No		N/A	
Location Data (Travel / GPS / GSM Data)		N/A	
Device MAC Address (Wireless Network Interface)		N/A	
Sensitive Personal Data			
Physical / Mental Health or Condition	Yes		The primary purpose of the RES-Q registry is collecting information about stroke care quality and providing feedback to hospitals. Therefore we collect clinical evidence of the treatment process, risk factors, lab results, logistics etc. of the patient.
Family / Lifestyle / Social Circumstance		N/A	
Racial / Ethnic Origin		N/A	
Genetic Data		N/A	

Data quality standards for personal data

Streamlining of datasets will help minimize data entry omissions. Comprehensive validation rules are built into the web-tool to ensure that incorrect, conflicting and/or illogical data cannot be saved.

Comprehensive help notes for each question will be provided and the questions themselves reviewed annually in order to ensure they are clear. The central team will operate a helpdesk to answer queries that arise. FAQ documents will be available for all audits. Data is periodically exported and checked centrally for any inappropriate cases or illogical data before analysis.

Unfortunately, currently there is no thorough audit for users or patients data either. Patient's data audit is not possible by RES-Q due to our global reach and limited personnel, but even now some hospitals that use RES-Q for certification are undergoing physical/online auditing by a local

committee. We would like to introduce user validation measures and random data audits with the help of national coordinators.

Details of registered webtool users will be audited periodically to ensure that we do not have out of date details. Users of RES-Q automatically receive important information, newsletters and surveys unless they unsubscribe.

Individual's rights

Individuals rights (where relevant)	Describe how you ensure individuals are aware of these rights	Describe how you would do this	Please copy and paste section of document that states the individuals rights
Individuals are clear about how their personal data is being used.	**Patient's data** A privacy notice is not yet available covering the whole programme. Posters and patient information leaflets will be made available online. **RES-Q registered users** Web-tool users voluntarily register themselves on the web-tool and are clear on the purposes for which their information will be used by the RES-Q team (administrative only). This is done via: ● emails during the registration process ● RES-Q privacy policies during registration.	**Patient's data** Privacy notice and patient information leaflets will be available via the RES-Q webpages (www.qualityregistry.eu) **RES-Q registered users** RES-Q users voluntarily register themselves and are clear on the purposes for which their information will be used by the RES-Q team (administrative only). Automated email is sent during the registration process to keep new users up to date. User details are not used outside of programme administrative activities (newsletters and customer support).	**Patient's data** Patients should be informed by their hospital that their data is going to be used in a pseudonymized manner in RES-Q. Privacy notice will also be posted on RES-Q website. **RES-Q registered users** Upon registering new users will receive an automated email to inform them that their registration request will be shared with the approver for their service (often a clinical lead) as part of one of the web-tool security measures.
Individuals can access information held about them	This will be included in the privacy notice. Generally, patients' identifiable information is not accessible to the RES-Q team. The only small exception is hashed National health insurance ID for patients using Outcome mobile app. RES-Q users identifiable information (name, e-mail, phone number) is accessible to the RES-Q team and users can change them in the RES-Q web tool.	In the majority of cases, we would not be able to provide the patient information held but would put the patient in touch with the hospital who would be able to help. Some patients using RES-Q Outcome mobile app will be identifiable for the RES-Q team by their National health insurance ID. RES-Q users can directly contact our team to request a change of their profile or do it themselves	Privacy Notice: *The right of access* You have the right to see what information is held about you. RES-Q Global is the only organization that receives users' personal data and pseudonymized patients' data. If you are a RES-Q user you can directly change your personal data in the RES-Q platform or let us know what you want to change. Generally, if you are a patient, we don't use identifiers like names and addresses so it is not possible for us to identify if you were included in the RES-Q registry. You have the *right to rectify* any data that is incorrect but rectifying it with us would not change the information in your RES-Q record and you may want to contact your healthcare provider directly. In some cases of patients using our Outcome mobile app RES-Q team can identify patients by their National health insurance ID and RES-Q team can respond to the *right to rectify* any data.

Individuals rights (where relevant)	Describe how you ensure individuals are aware of these rights	Describe how you would do this	Please copy and paste section of document that states the individuals rights
Request erasure (right to be forgotten) in certain circumstance, making clear that it does not apply to an individual's health or care record, or for public health or scientific research purposes	This will be included in the privacy notice. **RES-Q users data** Data is accessible only to the RES-Q team and the user. **Patient's data** Generally, patients' identifiable information is not accessible to the RES-Q team. The only small exception is National health insurance ID for some patients using Outcome mobile app.	**RES-Q users data** RES-Q users can ask us to deactivate their account. This will prevent them from using our services and entering data! Removal of user data is not possible due to auditing requirements, linking to activity on patients' records and database integrity. **Patient's data** In the majority of cases, we would not be able to provide the patient information held but would put the patient in touch with the hospital who would be able to help. Some patients using RES-Q Outcome mobile app will be identifiable for the RES-Q team by their National health insurance ID	Privacy notice: *The right to erasure* As a RES-Q user, you can request that we deactivate your account so nobody will be able to use your login information to access RES-Q services. Removal of user data is not possible due to auditing requirements, linking to activity on patients' records and database integrity. Please let us know by contacting us on this email: admin@qualityregistry.eu. Generally, if you are a patient, we don't use identifiers like names and addresses so it is not possible for us to identify if you were included in the RES-Q registry. You have the *right to rectify* any data that is incorrect but rectifying it with us would not change the information in your RES-Q record and you may want to contact your healthcare provider directly. In some cases of patients using our Outcome mobile app RES-Q team can identify patients by their National health insurance ID and RES-Q team can process the *right to rectify* any data.
Rectification of inaccurate information	This will be included in the privacy notice.	We can rectify inaccurate information for RES-Q registered users. Patients should contact the health provider that supplied the information to rectify at source. We can identify only patients using the Outcome app.	Privacy Notice: You have the right to see what information is held about you. RES-Q Global is the only organization that receives personal data of RES-Q users. If you are a patient, we don't have identifiable information about you (unless you use our Outcome app where we store hashed National health insurance ID). You have the *right to rectify* any data that is incorrect but rectifying it with us would not change the information in your health record and you may want to contact your healthcare provider directly.
Complain to the Office for Personal Data Protection	This will be included in the privacy notice.	Contact details for the Office for Personal Data Protection	**Contact the Office for Personal Data Protection** If you are unhappy with the way we handle your data or have dealt with a request, you have the right to lodge a complaint with the Office for Personal Data Protection at https://www.uoou.cz/ or phone +420 234 665 800.

Individuals rights (where relevant)	Describe how you ensure individuals are aware of these rights	Describe how you would do this	Please copy and paste section of document that states the individuals rights
Withdraw consent at any time (if processing is based on consent)	This will be included in the privacy notice. **Patient's data** RES-Q can react to informed consent withdrawal only in case of Outcome app project. Other patients must contact their hospitals if they signed informed consent. **RES-Q users data** Data is accessible only to the RES-Q team and the user.	**Patient's data** RES-Q can remove a patient's record only on request from hospital or on message from users of Outcome app. **RES-Q users data** User account modification of information can be accessed by logged-in users via RES-Q data collection platform.	Privacy notice: *Consent* Where people sign up to receive newsletters and updates, attend events or work with NACAP consent is received for us to store and process personal data. The Pulmonary Rehabilitation clinical audit collects patient data by obtaining consent from patients, as well as using Public Task and Special Categories of Data (ensuring high standards of healthcare). Information about the audit is provided to help clinicians obtain informed consent from patients. **RES-Q users data** Deactivation of user accounts can be done by contacting the RES-Q team at admin@qualityregistry.eu.
Data portability (if relevant)	This will be included in the privacy notice.	N/A	Privacy notice: *The right to data portability* If we do have information held about you (and we can identify you with the help of your hospital) and you wish to see it, we will provide your data in a format that you will be able to use, such as LibreOffice, Microsoft Office, RTF or CSV.
For data transfers outside the EU, a description of how the data will be protected.	This will be part of an agreement with participating hospitals worldwide.	RES-Q will enforce minimal data protection rules due to national legal diversity for data stored in RES-Q.	N/A
To know the legal basis under which their information is processed. Is there a clear legal basis for the processing of personal data? If so, what is the legal basis?	This will be included in the privacy notice, fair processing notices and the patient information leaflets.	Both the fair processing notices and patient information leaflets can be found via the RES-Q webpages (www.qualityregistrey.eu).	**Example from the primary care patient information leaflet** ***Why hasn't my doctor asked for my permission to use my information?*** *This doctor's neurosurgery department has agreed to take part in the RES-Q registry. The RES-Q registry will not collect any identifiable information. This means it is not necessary to ask for permission from each individual patient.*

Individuals rights (where relevant)	Describe how you ensure individuals are aware of these rights	Describe how you would do this	Please copy and paste section of document that states the individuals rights
			(continued from the previous page) From the Privacy Notice: **Our legal basis for collecting information** The legal bases for collecting and using personal data are: *Public Task* We collect only the information that is necessary to carry out our function and avoid collecting information that will not be used. This is received from healthcare providers. To see what information is held in your healthcare record please contact your hospital. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. *Consent* Where people sign up to receive newsletters and updates, attend events or work with RES-Q, consent is received for us to store and process personal data. *Contract* For example, this is the basis we use when it is necessary for us to take specific steps before entering into a contract with you to supply you a service or vice versa. *Legal obligation* For example, this is the basis we use when it is necessary for us to comply with the law (not including contractual obligations) because we are required to keep documentation to produce in court proceedings. *Legitimate interests* This basis is used to allow us to hold information as evidence should we need it in the future, for example, if you ask us to unsubscribe you from our newsletter. *Common Law Duty of Confidentiality* Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
To know the purpose(s) for the processing of their information.	This will be included in the privacy notice, the fair processing notices and patient information leaflets include information on this.	The fair processing notices, privacy notice and patient information leaflets can be found via the RES-Q website.	**Example from patient information leaflet** *Linking the data in this way allows us to look at more aspects of your care without asking hospitals to enter extra information into our database.*

Individuals rights (where relevant)	Describe how you ensure individuals are aware of these rights	Describe how you would do this	Please copy and paste section of document that states the individuals rights
Whether the provision of personal data is part of a statutory obligation and possible consequences of failing to provide the personal data	N/A	N/A	N/A
The source of the data (where the data were not collected from the data subject)	The patient information leaflets provide this information.	Patient information leaflets will be made available on the RES-Q webpages (admin@qualityregistry.eu)	**Example from patient information leaflet** ***Where does my confidential information go?*** *The **hospitals taking part** in the RES-Q register will **enter information about your care, along with your confidential information, into a highly secure online database**. This is held by RES-Q Global (FNUSA-ICRC), which follows best practice in data protection and security. **It will be held indefinitely.*** *Staff at RES-Q will only see personal details for database administration and* *have to follow strict confidentiality rules.*
Categories of data being processed	Datasets and data flows.	Patients' datasets and data flows will be made available on the RES-Q webpages for RES-Q users. Data flows will be color-coded to enable easy identification of what category of information each flow falls into (raw, pseudonymised and aggregated)	Please note the following: Stroke care information is available on www.qualityregistry.eu Information will include datasets and data flows which will outline all categories of data being processed by RES-Q.
Recipients or categories of recipients	Datasets and data flows.	Data flows will be available on the RES-Q webpage. All data flows include information on data processes and controllers for each stage of the process.	Stroke care information is available at www.qualityregistry.eu Information includes data flows which will outline all recipients or categories of recipients who receive patients' data.

Individuals rights (where relevant)	Describe how you ensure individuals are aware of these rights	Describe how you would do this	Please copy and paste section of document that states the individuals rights
The source of the personal data	The privacy notice and patient information leaflets provide this information.	Patient information leaflets will be available via RES-Q webpage (www.qualityregistry.eu)	**Example from patient information leaflet** **Where does my confidential information go?** The hospitals taking part in the RES-Q registry will enter information about your care, along with your confidential information, into a highly secure online database. This is held by RES-Q Global NGO, which follows best practice in data protection and security. It will be held for the duration of the registry. Staff at RES-Q will only see personal details for database administration and have to follow strict confidentiality rules. Example from the privacy notice: The audit information will be linked with data already held by ÚZIS.
To know the period for which their data will be stored (or the criteria used to determine that period)	As above	As above	As above
The existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on data subjects (if applicable)	N/A	N/A	N/A

Privacy Risks

Types of Privacy risks

- Risks affecting individuals or other third parties, for example; misuse or overuse of their personal data, loss of anonymity, intrusion into private life through monitoring activities, lack of transparency.
- Compliance risks e.g. breach of the GDPR
- Corporate risks (to the organization), for example; failure of the project and associated costs, legal penalties or claims, damage to reputation, loss of trust of patients or the public.

Risks affecting individuals

Patients have an expectation that their privacy and confidentiality will be respected at all times, during their care and beyond. It is essential that the impact of the collection, use and disclosure of any patient information is considered in regards to the individual's privacy.

Pre-hospital care

As prehospital care collects only aggregated data instead of individual patient data, there are no individuals, whose data can be potentially at risk.

Hospital care

Patients admitted to hospital with stroke symptoms in hospitals using RES-Q worldwide. There is data of 416,000 patients at the end of 2021. We would hope the dataset would increase by approximately 100,000 per annum.

Currently there are no patients with pseudonymous personal id at the end of 2021. In such a case RES-Q patient data itself doesn't allow to re-identify patients. It would also be necessary to acquire data from the hospital's Electronic Healthcare Records.

Only a very limited subset of patients data in RES-Q will contain a pseudonymized personal identifier in the near future.

Potential number of affected patients = 416,000 by the end of 2021, mostly from Thailand, Vietnam, Poland, Czech Republic, Ukraine and Bulgaria

Impact: all patients with pseudonymized personal id in RES-Q will be at risk, risk of the others is very limited

Post-hospital care

All patients discharged after stroke in the Czech Republic, will start to use the mobile application to monitor their quality of life. Every patient will be identified by pseudonymous personal identifier. This component should be available in 2023.

Impact: all patients data are at risk

Number of individuals (users and contacts) on RES-Q platform = 3,000 unique users/contacts currently. This is likely to increase as soon as pre-hospital care and post-hospital care components will be publicly available.

When assessing the potential risks affecting individuals we considered that:

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organizations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously. This will influence only a small portion of patients using the Outcome app.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information. Children or patients heavily disabled after the stroke can exercise their rights via their caregivers only.
- Collecting information and linking identifiers might mean that an organization is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Organization and compliance risks

Possible corporate risks include:

- Non-compliance with the GDPR or other legislation can lead to sanctions, fines and reputational damage.
- Potential risk is starting a legal dispute or proceeding with another led by a supervisory authority from another country.
- The use of National health insurance ID or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organization.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the quality of stroke care.
- Public distrust about how information is used can damage an organization's reputation.
- Data losses will not damage individuals rights.

Possible compliance risks include:

- Non-compliance with the GDPR.
- Non-compliance with the privacy and healthcare laws, cyber-security regulations.
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.

Managing Privacy and Related risks

We considered many different steps to reduce identified privacy risks, including:

- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely pseudonymize the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests as mentioned above, FNUSA will introduce a SW

system, which will simplify processing of requests from subjects.

- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organization for assistance if necessary.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

Based on new project plans detailed information, we can identify more precisely how a general risk may occur.

Privacy Risks and Actions Table

Please see appendix 2 for additional guidance on completing this table

What are the potential risks to the individuals whose personal data you hold?	**Likelihood of this happening** 1 Very unlikely 2 Unlikely 3 Possible 4 Likely 5 Very likely (See guidance below for definition)	**Impact** 1-Insignificant 2-Minor 3-Moderate 4-Major 5-Catastrophic (See guidance below for definition)	**Overall risk score** (likelihood x impact = score)	**Will risk be accepted, reduced or eliminated?**	**Mitigating action to reduce or eliminate each risk** **OR** **Where risk is accepted, give justification.**	**Explain how this action eliminates or reduces the risk**	**Expected completion date**	**Responsible owner**
Illegitimate access	2	5	10	Reduced	FNUSA holds all identifiable information. Nobody else has access to these identifiers. Only nominated individuals have access to the data, and only the individual hospitals themselves can see the patient identifiable data of their own patients. Access to the database is via secure client software, operating over a secure VPN. Currently hospital data storage has no ISO 27xxx certifications. Potential risk is that users by registering themselves into the hospital get access to data of all patients treated in this center.	These measures ensure that the risk of an illegitimate is low. Because of Cyber Security Act which is now binding for FNUSA hospital data storage will have ISO/IEC 27 000 certifications family in 2022. Transfer of the RES-Q platform to external hosting with a secure data center with ISO 27001, 27017, 27017 certifications which are compliant with healthcare data hosting legislation in a number of countries including France, Germany, Italy, Poland and the UK.		
Undesired modification	2	4	8	Reduced	Same as above	Same as above		

What are the potential risks to the individuals whose personal data you hold?	**Likelihood of this happening** 1 Very unlikely 2 Unlikely 3 Possible 4 Likely 5 Very likely (See guidance below for definition)	**Impact** 1-Insignificant 2-Minor 3-Moderate 4-Major 5-Catastrophic (See guidance below for definition)	**Overall risk score** (likelihood x impact = score)	**Will risk be accepted, reduced or eliminated?**	**Mitigating action to reduce or eliminate each risk** **OR** **Where risk is accepted, give justification.**	**Explain how this action eliminates or reduces the risk**	**Expected completion date**	**Responsible owner**
Illegitimate access to dataset during the data transfer	1	5	5	Reduced	Users are able to download a dataset which contains only patient data for their hospital or country (national coordinator). This transfer is secured by https and only logged users can do so. Therefore sending of any dataset in email attachment will be reduced only to exceptional cases. Datasets will contain de-identified patient data instead of preprocessed patient data.	Further reduction of dataset transfers over email will reduce the risk that dataset will be sended to an incorrect email address. Transfer of de-identified data will reduce the impact of illegitimate access.		
Data breach (leakage)	2	4	8	Reduced	As users can download preprocessed patient data it's possible that unintentional data leakage happens e.g. by careless disposal of used computer equipment or data storage media. In future users will be able to download only de-identified patient data instead of preprocessed patient data.	This reduces the impact of such a data leakage.		
User from hospital A can access data of hospital B without authorization	1	4	1	Reduced	Refactoring of data collection user interface with more robust and secure technologies.	Usage of more robust and secure technologies on user interface will reduce likelihood that logged user will be able to access data without authorization.		
Disappearance of data	1	3	3	Reduced	RES-Q Global backed up all user data on a different secured server. RES-Q can delete patient data, but it is recommended (to protect database integrity and for auditing purposes) instead to mark them as "deleted" which only prevents their further processing.	Security systems ensure that all data is held safely and the risk of disappearance or loss of information is at an absolute minimum.		

What are the potential risks to the individuals whose personal data you hold?	**Likelihood of this happening** 1 Very unlikely 2 Unlikely 3 Possible 4 Likely 5 Very likely (See guidance below for definition)	**Impact** 1-Insignificant 2-Minor 3-Moderate 4-Major 5-Catastrophic (See guidance below for definition)	**Overall risk score** (likelihood x impact = score)	**Will risk be accepted, reduced or eliminated?**	**Mitigating action to reduce or eliminate each risk** **OR** **Where risk is accepted, give justification.**	**Explain how this action eliminates or reduces the risk**	**Expected completion date**	**Responsible owner**
Network failure	3	1	3	Reduced	As RES-Q doesn't provide any realtime service for its users network failure means just temporary service unavailability. Patient data can be stored or evaluated after network failure recovery without any impact on healthcare. All data is stored on persistent storage and regularly backed up, therefore network failure doesn't lead to any data disappearance. Nowadays RES-Q rely on FNUSA network.	Transfer of the RES-Q platform under RES-Q Global and services to external hosting with guaranteed availability will reduce the risk of network failure.		
Cyber-attack (DDoS)	1	1	3	Reduced	Transfer of RES-Q platform outside of hospital's infrastructure.	Hospitals are common targets for cyber-attack. Transfer of RES-Q outside of the hospital (FNUSA) infrastructure will eliminate the risk of being affected by cyber-attack on the hospital. Therefore the overall likelihood of being a target of cyber-attack will be reduced.		
Data platform malfunction	2	3	6	Reduced	Validation and certification of used technology should minimize any platform malfunction. OpenClinica is open-source software and it was already validated and certified by various organizations. (https://www.openclinica.com)	Data collection platform OpenClinica was validated and certified (https://www.openclinica.com/). Changes introduced by the RES-Q team to the code concern only UI and graphics of the software and are documented. They didn't affect any data processing.		

What are the potential risks to the individuals whose personal data you hold?	Likelihood of this happening 1 Very unlikely 2 Unlikely 3 Possible 4 Likely 5 Very likely (See guidance below for definition)	Impact 1-Insignificant 2-Minor 3-Moderate 4-Major 5-Catastrophic (See guidance below for definition)	Overall risk score (likelihood x impact = score)	Will risk be accepted, reduced or eliminated?	Mitigating action to reduce or eliminate each risk OR Where risk is accepted, give justification.	Explain how this action eliminates or reduces the risk	Expected completion date	Responsible owner
Organization risks & compliance risks section								
Mass individual right requirements under GDPR	1	3	3	Accepted	There is a risk that patients who have opted-out of having their patient identifiable information used for quality improvement/research purposes will be anyway entered into the RES-Q. Responsibility for not entering that patients' data is solely with the hospital that is entering the data.	Clear information during registration and educating RES-Q users by webinars or leaflets on RES-Q website should ensure that hospitals will follow these requirements.		
Records of Processing activities	3	2	6	Accepted	Under article 30 GDPR there is an obligation to record and annually update processing activities. Currently we are not able to comply with this requirement, but in 2022 we will introduce a software solution to deal with this.			

DPO Statement

the DPIA be passed to the Data Protection Officer for Approval? **If not please state the reason why and return the form to the lead who completed it.**	**Yes** **No**		**Click here to enter text.**
DPO Advice Provided **Yes** **No** **NR**		**Date**	
Summary of DPO advice:			
DPO advice accepted **Yes** **No** **N/A** ***(If no state reason why below)***			
Comments:			
Residual High risk **Yes** **No** ***(if yes report to ICO before proceeding)***			

ICO Outcome:	
Approvals	
DPIA Approved	**Yes No** ***(if no state reasoning why below)***
Approved By	
Title	
Signature	
Date	
Reasoning for rejection:	

DPIA Review Due Date		**DPIA Owner**	

Regularly reviewing the DPIA

This DPIA is an ongoing process and it shall be regularly reviewed during the lifecycle of the project to ensure

- Risks identified are still relevant
- Actions recommended to mitigate the risks have been implemented and mitigating actions are successful