H2020-MSCA-ITN-2018-813545

HELICAL

Health Data Linkage for Clinical Benefit

Deliverable 4.4

Proposed governance framework for research in rare diseases

Introduction

This deliverable proposes a governance framework which can act as a “tool kit” that may be used by European projects conducting research in rare disease areas. Its main aim is to provide a governance framework which facilitates the adoption of consistent, legally and regulatorily compliant practices for all research studies between partners and sites.

The instruments (policies, codes, rules, assessments and template agreements) being defined and listed below for governing the conduct of research have been designed, and were regularly updated, as part of the HELICAL project to ensure that the autonomy and decision-making of each data/sample source was respected, including adherence to any local governance arrangements the source may be obliged to follow. Coupled with the Governance framework of the project (Deliverable 4.3) and the Information Governance Policies (Deliverable 4.2), the data governance framework has been informed by the activities described in these deliverables and represents their implementation, which are envisioned and proposed to act as guidelines and tools that can be used in further projects and research.

The General Data Protection Regulation (GDPR) establishes the paradigm of “data protection by design and default” where protection of data needs to be considered and built in from the outset of developing any data intensive activity; this was established as a first requirement for the development of the HELICAL governance framework. The second requirement, embodied in the purpose of a Data Protection Impact Assessment (DPIA), was to run an impact assessment for any processing of data to assess whether there were particular risks to the rights and freedoms of individuals, and to the controllers and processors of data required to achieve the particular intended purpose.

This deliverable therefore explains the information governance steps, processes, documentation and legislation (both current and upcoming) that a research consortium should develop, populate and adhere to in order to undertake collaborative research in a rare disease area that includes genomic information. These framework steps take the form of a:

- Data Management Plan,
- Project wide DPIA (as well as separate DPIAs undertaken by each consortium partner),
- Material and Data Sharing Agreements as well as a
- Consortium information governance policy, all of which are included in Deliverable 4.3.

This document concludes with a discussion of forthcoming EU Regulations that are further shaping the health data research and innovation sector and likely impacts on governance arrangements. This includes the new data altruism mechanisms and consent requirements.

Proposed Governance Framework Details

The advent of GDPR led to a series of tools that would help identify Data Protection risks and allow any organisation processing personal data to explore these risks and take action to ensure that they were mitigated. The premise of these tools was around the protection of data but also to ensure its flow according to the GDPR Principles.

The HELICAL risk management approach used these tools. They are associated with GDPR's Data Protection by Design and Default paradigm, which is an approach for building in data protection from the very beginning of any data intensive activity. This is no less the case for research projects, especially those involving vulnerable participants and rare diseases where the population is comparatively small and protection measures such as anonymity are therefore harder to achieve.

The key governance aspects to achieve a robust and accountable framework for rare disease research discussed in this section are as follows:

1. General Approach – Data Protection by Design and Default;
2. Training and Educational Needs;
3. Project Wide and Partner Organisation DPIAs;
4. Project Data Management Plan;
5. Policies and Codes of Practice Development.

Please note that full details of these aspects can be reviewed across the WP4 Deliverables.

General Approach – Data Protection by Design and Default

As part of Data Protection by Design and Default, a Data Protection Impact Assessment (DPIA) is a tool that can be used to impact assess against the risks to data protection compliance. Using a template that is in line with Supervisory Authority Guidelines, a DPIA template developed by i~HD experts has been used, because it is designed with secondary uses of health data (i.e. innovation and research) in mind. This DPIA template is available in D4.2.

An information governance board that comprised all project partners, including the Patient Association Organisations, oversaw this process. ESRs were also required to report to the board, as well as provide presentations to the PAOs about their research and how they were protecting the data.

In order to achieve the approach, it is important to engage with all project partners and encourage them from the outset to think about data requirements, tooling and flows early on, ideally at the point of consortium agreement negotiation. This can be achieved by workshops, training stand education sessions and / or questionnaires and interviews.

Training and Educational Needs

The approach also requires that a research project ensures the adequate training and education of its teams. This involves making sure they are fully aware of research governance training as well as how to protect data and understand data protection requirements and safeguards. To that end, HELICAL arranged for training and education workshops around GDPR and Research Governance requirements for handling data.

The full details are available under Deliverables 4.2 and 4.3 but the workshops required Early-Stage Researchers to develop their own DPIAs to fully understand the GDPR and wider Governance requirements whilst gaining practical experience for governance tools. This also ensured that they were thinking about their data requirements and flows from an early stage in their project design and implementation.

Project Wide and Partner Organisation DPIAs

The approach also recognises that regulatory compliance across all partners in a research project is essential. This is harder in a large consortium of partners who are working together across European countries with data to ensure the research goals in a project are met. Conducting a project wide DPIA is therefore essential to support individual partners achieve their compliance goals. Whilst a project wide DPIA itself has no legal standing as a consortium is not a legal entity, the individual partners that make up that consortium are legal entities and have their own regulatory requirements to meet, including running a DPIA or explaining why they believe one is not necessary for the record and for inspection by Supervisory Authorities. A project wide DPIA is therefore very useful to provide the key details of the project and inform the Partners' own DPIAs, and to assure a degree of consistency in risk assessment across the partners.

Project Data Management Plan

In developing the DPIAs, in parallel a further governance element is the Data Management Plan. For publicly funded research projects, these plans must be completed and made available publicly. These plans require that projects specify the data items they will be using, and how they will make these available under the Open Science Initiative, if at all. Additionally, the project must specify how they will adhere to the Findable, Accessible, Interoperable and Reusable (FAIR) Principles and indicate costs, or whether they will not adhere to them with an explanation. These principles are designed to ensure that the maximum utility can be gleaned from data assets that are supported by public funding and that value can be realised for public benefit as fully as possible.

In any event, the Data Management Plan (DMP) also requires that a specification of how data will be secured is published, which further helps projects to define their security requirements (or the initial high level requirements at least) early on in the project lifecycle.

Policies and Codes of Practice Development

Through the process of conducting the DPIAs for the project and each of the ESR individual studies, HELICAL was able to obtain a clear picture of the governance requirements and where policies and codes of practice would be needed. The precise details of these could also be established based on the DPIAs and the assessment frameworks. These are available under D4.3.

New and Upcoming legislation

The GDPR is one of the primary pieces of European legislation which, in association with other European and national compliance and privacy regulations, represents the regulatory framework that HELICAL and other European funded projects engaging in sharing and processing of personal data need to adhere to. At the time of drafting this deliverable, the following legislative proposals proposed by the European Commission, and listed below, have high relevance, and would also need to be considered when engaging in research projects that include the secondary use, processing and handling of personal data in healthcare.

Medical Devices Regulation (MDR)

The adoption of the new MDR came in May 2021, thereby replacing the previous Directive. The European Commission described the aim behind the newly updated MDR, which entered into effect after a long awaited four-year transitional period that was extended due to the Covid-19 pandemic, to be the alignment of "EU legislation […] with technical advances, changes in medical science and progress in law-making". This modernisation of the regulatory EU medical devices framework brings with it many changes, including a life cycle-approach regarding medical devices as well as a new risk classification system for medical devices and more transparency and better traceability of medical devices following the introduction of the Eudamed database and the Unique Device Identifiers.

Considering this as well as the obligation of manufacturers and EU representatives to appoint a person responsible for regulatory compliance, the framework and classification system contained within the MDR needs to be considered when engaging in research which will, or may have, as a deliverable the creation of a product or tool which may fall within the definition of a 'medical device' under the MDR. The design, implementation and evaluation requirements of the MDR should be taken into account even if it is not intended to seek formal certification during the project lifetime. A number of those requirements need to be met from the start of the development process and are difficult to retrospectively evidence after a project has ended.

Data Governance Act (DGA)

Presented in November 2020, the DGA was the first proposal to be announced as part of the European Commission's 2020 European Data Strategy and has since been adopted by the

eventual agreement of the European Parliament and the Council of the EU in May 2022, although not yet enacted.

The DGA, which is to work in conjunction with the GDPR, has as its aim to increase the amount of data, such as healthcare data, available for re-use within the EU by allowing public sector data to be used for purposes other than the ones for which the data was originally collected. The Act proposes the creation of sector specific data spaces to promote and facilitate the sharing of data within these spaces, which also include a health specific sector. Further, under the DGA the Commission introduces data sharing bodies called “data intermediaries” which will handle the sharing of data by individuals, public bodies and private companies. To this end, the DGA introduces the now codified concept of “**data altruism**”, which aims to encourage individuals to voluntarily donate personal data to serve the general interest and a framework is presented in order to ensure that the data shared will be used for the agreed purposes, which scientific or medical research would for example fall under. Organisations which therefore engage in activities as the ones listed under the DGA would classify as “data altruism organisations”, for which a certification can also be provided.

AI Act

The AI Act, the first regulating act targeting artificial intelligence, was proposed in April 2021 and aims to harmonise rules regarding AI applications, ensuring safety and fundamental rights protection. The proposal itself stems from the White Paper on AI, published in February 2020, which proposed to set up a European regulatory framework for trustworthy AI. As it currently stands, the Proposal is being discussed by the co-legislators, the European Parliament and the Council, with the Parliament report to have more than 300 amendments to be considered and discussed.

The AI Act proposal, similar to the DGA, explicitly states that the Act is meant to work in conjunction with the GDPR to ensure compliant data handling and data protection. It aims to enshrine in EU law a technology-neutral definition of AI systems and assigns applications of AI to four risk categories: applications and systems that create an unacceptable risk, such as government-run social scoring; high-risk applications, such as health and educational interventions, CV-scanning tools that rank job applicants; limited and minimal risk AI.

Considering the ‘horizontal’ nature of the Act, once adopted and implemented, its complexities will cut across varying sectors and thus may have direct applicability to consortia which wish to undertake medical research in genomics and will or may use and develop AI systems.

European Health Data Space (EHDS)

The EHDS was introduced by the Commission in May 2022 with its purpose to regulate the sharing of health data across the EU for private individuals, researchers or policymakers and aim to have the implementation of the Regulation running in 2050. The proposal is currently still being discussed at Council level.

The Regulation has a twofold objective, on the one hand to give control to European citizens of their health data (listed under the proposal as ‘primary use of health data’), including regarding cross borders purposes, and on the other hand at facilitating the uptake of the re-use of health data (‘secondary use of health data’) for research while simultaneously ensuring compliance with the EU data protection standards. In that regard, working alongside the GDPR, the Regulation proposal establishes a set of rules and infrastructures to support these as well as a European governance framework.

Broad consent and data altruism

An on-going issue that researchers have been faced with when reusing data which were obtained by patients based on Article 6(1)(a) GDPR is that “consent” as a legal basis has requirements which need to be met and are difficult in practice to achieve, particularly in the context of scientific research. This field has been explored, commented and analysed by both stakeholders, academia as well as the European Institutions and, in spite of guidance obtained by the European Data Protection Board and Supervisor, without an eventual solution.

As described in page 7 of the Deliverable, the DGA has established the concept of ‘data altruism’ as a pathway through which, alongside the GDPR legal basis, individuals and/or organisations may be able to donate and thus reuse data for research. This then begs the question as to whether the concept of ‘data altruism’, and the associated framework proposed under the Regulation, is the solution industry and consortia have been waiting for.

Although the mechanism for a common European data altruism consent form is proposed in the DGA and explicitly mentions the GDPR compliance that this exercise needs to adhere to in practice, the issue of consent does not seem to be resolved, rather it is attempted to be circumvented and then becomes highlighted. The preamble to the proposal, as it currently stands, states that “data altruism would rely on consent of data subjects in the sense of Article 6(1)(a) and 9(2)(a) and in compliance with requirements for lawful consent in accordance with Article 7” of the GDPR. Further, Article 22(3) of the proposed Regulation states that, where

personal data are provided, data subjects can give and withdraw consent according to GDPR requirements under the European data altruism consent form. This therefore translates in practice that although the avenue proposed for ‘data altruism’ may sound promising, in the end it relies on specific and informed consent, just as it has been outlined under the GDPR, and therefore implies and carries the same limitations that have existed so far when the secondary uses of the data involved is needed for future looking research. As stated above, the proposal is still pending enactment which may bring with it further clarification and guidance on the topic as well as guidance from the Court of Justice of the European Union.

Concluding Remarks

HELICAL presented unique governance challenges around data and its protection. The key aspects described in this Deliverable carry equal weight in terms of being able to successfully govern rare disease research from the data perspective.

From the training and educational perspective, the project focus has been on upskilling ESRs and their abilities to understand and work with governance arrangements for their research represents a key requirement for them as part of their skills repertoire. The project has given an opportunity for them to learn from experts and put their learning into practice.

From the risk management perspective, the GDPR mandated approaches of Data Protection by Design and Default and DPIAs have meant that all project teams have been able to develop this toolkit and protection measures that have the best chance of achieving compliance, protecting data, and defending the decisions where necessary. They have given rise to, among others, a DMP, policies and codes of practice.

This toolkit has been developed amid a rapidly developing regulatory landscape across the EU and beyond. The Deliverable has therefore been written to adapt to each of these new regulations as they emerge and are enforced. It lists the key pieces of regulation where they have been designed to work alongside GDPR. Ensuring that the toolkit remains usable in this context of developing regulations for future proofing relies on its basis in GDPR. It will likely need to be reviewed periodically to ensure it remains in line with developing legal decisions and as cases are heard and precedents set.