Manuscript legal agreements templates

Legal agreements for using health-related data in multi-center projects

J. Maurer, Personalized Health Informatics Group (PHI), SIB Swiss Institute of Bioinformatics

The following manuscript outlines legal agreements and their principle content, which needs to be considered when conducting multi-center research projects in Switzerland, not only in the context of the Swiss Personalized Health Network initiative.

Requirements for research projects in Switzerland

Planning and conducting research projects with health–related data imply certain requirements postulated by the ethical and legal regulations. Depending on the developed project plan for most of the health-related data collected from patients within hospitals, the patients' consent for further usage of their data and the accompanying ethical approval is needed. For the purpose of further use of data, patients' consent is often collected in form of a general consent. The possibility of providing a general consent has already been implemented in many Swiss hospitals, and allows the further use of data for not yet defined research projects according to the Human Research Act (HRA) Art. 32ff. Typically, data are pseudonymized (coded) following consolidated de-identification rules before using respectively sharing data with other institutions or hospitals in multi-center research project. Some projects use anonymized data that do not fall within the scope of the HRA. However, it is strongly recommended to still apply for an ethical statement describing the purpose of anonymization and its process in detail.

Another important requirement is to establish a legal framework, which defines the project specifications and responsibilities of participating partners in compliance with Swiss legal regulations and data protection requirements. This kind of framework is described in a Consortium Agreement (CA) and completed by a Data Transfer and Use Agreement (DTUA). The CA regulates general principles of collaboration between research project partners, such as the rules for publication and authorship, intellectual property, financial conditions and governance aspects. The DTUA describes specifically under which conditions the data provider (e.g. hospital) agrees to disclose patients' data to a recipient (e.g. a university). In addition, the agreement indicates technical security measures for processing health-related data, which for example prevent unauthorized persons to access the project data.

Overview legal agreements for research purposes

As indicated before it is crucial to establish a contractual framework when conducting a research project with several centers/institutions. In general, the following legal agreements can be considered for multi-center projects with health-related data:

- Consortium Agreement (CA)
- Data Transfer and Use Agreement (DTUA)
- Data Transfer and Processing Agreement (DTPA)
- Material Transfer Agreement (MTA)
- Service agreements (with labs, software developers, etc.)

These types of agreements can be set up as stand-alone agreements or combined with each other, depending on the already existing contractual relation among the project partners.

The updated templates are available on the SPHN webpage https://sphn.ch/services/dtua/. Note that the developed templates are also applicable for projects not funded by SPHN, but there might be the need to adapt some clauses accordingly. For projects not using the BioMedIT infrastructure, a DTUA without external processor is provided. An MTA template is available on the webpage of the Swiss Biobanking Platform (SBP) https://swissbiobanking.ch.

SIB Swiss Institute of Bioinformatics
Personalized Health Informatics Group (PHI)
Elisabethenstrasse 43
CH-4051 Basel

History of harmonized legal agreements for sharing data

The templates available on the SPHN webpage are templates that have been further developed by the SIB Swiss Institute of Bioinformatics. Initially, one of the templates, the DTUA, was a result of an SPHN National Working Group, a collaborative group with representatives of universities, hospitals, SIB and SBP in the realm of the SPHN initiative. The initial template had to be updated according to the needs of SPHN projects using data processors, i.e. the BioMedIT nodes. With this revision, remaining aspects were covered, such as minimal security requirements or information and audits of security measures. In November 2020, templates for a CA, a DTUA and a DTPA including all remaining updates were released and published on the SPHN webpage https://sphn.ch/services/dtua/.

Consortium Agreement (CA)

Each of the agreements regulates specific aspects for using health-related data and can be set up, as mentioned earlier, as stand-alone agreement or combined. The consortium agreement regulates the general principles of collaboration between the research partners, mainly negotiated between the principal investigators of each participating institution/hospital. It defines the principles of collaboration and data exchange, governance and financial aspects, confidentiality, as well as intellectual property rights, publication and authorship.

Data Transfer and Use Agreement (DTUA)

If health-related data is used from several hospitals in a multi-center project, Swiss hospitals must set up a DTUA, which describes under which conditions the data provider (e.g. a hospital) discloses data to the recipient (e.g. a university). Originally, each data provider is controller of its own data. Once the data are collected and processed in such way that multiple institutions decide together why and how they process certain data, they become joint controllers of these data (meaning they are responsible together for these data). However, parties can decide that certain parties of the consortium will not determine the purpose of the data processing (e.g. a party will only provide technical/analysis help). All research partners or their institutional representatives involved in the transfer and use of data are part of the DTUA and must sign.

BioMedIT network

As integral part of the SPHN initiative, the PHI Group of SIB established the BioMedIT network, based on three BioMedIT nodes, building a coordinated infrastructure for secure processing of biomedical data. The three nodes are located in Basel (operated by the University of Basel's sciCORE Group), Lausanne (jointly operated by University of Lausanne and SIB) and Zurich (operated by ETH Zurich's SIS Group).

Typically, SPHN funded projects set up a defined project space with a secure (high-performance) computing environment for the project specific generated data set. Data coming from different data providers (hospitals) are transferred, depending on the affiliation, via the BioMedIT nodes to the project specific space of the main BioMedIT node and accessed remotely (e.g. via the BioMedIT portal). Data Transfer and Processing Agreement (DTPA)

By using this infrastructure, the controllers of the project's data (data providers and recipients) subcontract the secure transfer and processing of data to a third party (processor). To regulate the relationship between the data controller of the research project and the processors, a DTPA is set up. It defines data access rules and minimum security requirements. The processor acts as subcontractor according to the instructions of the controller.

Defining the roles of research partners

In some cases, it is not clear which of the legal agreements needs to be chosen. It helps to clarify that question by defining the roles of the research partners. Here is a first, simple example: There are two data providers, university hospitals A and B, sharing patients' data with a university X, the data recipient.

To show the different roles, it is worth to highlight who discloses data to whom (data provider) and who is accessing the data (data recipient). In the example, both universities share data with the recipient and access also project data.

Moreover, it needs to be define controllership (data controller).

When the purpose and manner of processing project data are determined jointly by all partners, the data provider and data recipient act as joint controllers. Hosting and processing of data might be subcontracted to a third party, e.g. to the BioMedIT network.

The set-up of the legal framework starts with the regulation of general principles of collaboration and data usage, for which a consortium agreement (CA) might be developed.

Within this agreement governance and financial aspects, intellectual property rights and the regulation of publications are negotiated between the research partners. The partners may arrive at an agreement that the intellectual property is jointly owned by the parties.

To regulate the conditions under which data are disclosed to the other party, a Data Transfer and Use Agreement has to be set up between the research partners. In this case as an integrated part of the CA.

If the processing of data is provided as service by a third party, in this case by the BioMedIT network, a Data Transfer and Processing Agreement needs to be concluded between the respective partners. The processing agreement regulates services for a secure and safe hosting of data and data access rules.

Which of the three BioMedIT nodes (Basel, Zurich and Lausanne) have to be subcontracted in which role depends on the site of the data providers, the location of the University X and the services to be provided.

One of the nodes, the "main node" (it could be the Basel node) provides a secure project space and compute power for data analysis, whereas the other nodes might serve as "transferring nodes" only.

In the SPHN context, data provider and data recipient often mandate the processor, the BioMedIT node(s), together.

Security measures

The other security measures mentioned are technical and organizational measures that ensure the confidentiality, integrity, availability and resilience of the systems with regard to processing of the project data. The provided measures are the responsibility of the recipient and ensure, for example, that:

- unauthorized persons are not able to access data processing system
- unauthorized persons are not able to read and delete data in the system or during transport of data
- examination and verification when and by whom data was entered in to system is guaranteed
- adequate organizational measures to protect data are established

For SPHN funded projects, the Information Security Policy (ISP) provides management direction and support for information security in accordance with SPHN requirements and respective legal regulations. It provides control mechanisms ensuring confidentiality, integrity and prevent misuse.

Use case of a multi-center research project using data from 3 hospitals and BioMedIT network

To clarify the roles of research partners and the agreements made between them, a use case is presented in the following. It is a research project with four research partners using health-related personal data from three Swiss university hospitals: The University Hospital Basel (USB), the University Hospital Bern (Insel Gruppe AG), and the University Hospital Geneva (HUG);ETH Zurich collaborates as research partner. All partners are using the BioMedIT network, consisting of the BioMedIT nodes Basel, Zurich and Lausanne.

- Defining the roles of the parties

Each of the three hospitals provides health-related personal data using the BioMedIT network for a secure data transfer and analysis.

In this use case the “main node”, the place for hosting and analyzing the project data, is the Zurich node. The Basel and Lausanne nodes act as “transferring node” only. All data are transferred to the main node and its defined project space. The project partners have concluded a separate (service level) agreement with the Zurich node with regards to the required services (e.g. storage and compute capacity, software requirements, etc.).

Access to data on the defined project space located at the main node is given to all research partners. Thus, all parties are data recipients.

In the use case, project partners determine together the means of data processing and act as joint data controller.

- Set up of CA incl. DTUA+DTPA

Once all roles are defined the legal framework can be built. To regulate the principle of collaboration and data exchange, governance and financial aspects, confidentiality, as well as intellectual property rights, publication and authorship a consortium agreement is set up among the data controllers.

To define the conditions under which data is disclosed to the parties, a DTUA among the research partners is integrated to the CA.

The controllers of the project’s data (data providers and recipients) wish to subcontract the secure transfer and processing of data to the BioMedIT network. The DTPA describes the data and services provided and is as an ANNEX added to the DTUA and approved and acknowledged by the project partners.

Finally, the legal agreements for sharing the data, consisting of a CA and an integrated DTUA and DTPA is settled. Once it is signed, data can be shared among the parties.

A full-fledged DTUA with external processor

Depending on the configuration of the research project, it might be sufficient to use a DTUA with an integrated DTPA only, for example, if there is already a signed CA or equivalent for the project. If the research partners decide to cover the legal framework with a DTUA and DTPA only, principle regulations of governance, confidentiality, intellectual property rights and publication must be covered in the DTUA. For projects not having any legal agreement among the partners, however, a full agreement framework constituting of a CA with an integrated DTUA and DTPA is recommended, but this depends on the project specifications.

A full-fledged DTUA without external processor

For multi-center projects, which are not part of the SPHN initiative and not using the BioMedIT network, a DTUA without processor (BioMedIT network) might be used. In this case, the project partners have to

ensure that the infrastructure on which the data is processed fulfills the requirements regarding information security.

A DTPA only

If there is only the need to cover terms and conditions for the use of a processing infrastructure such as the BioMedIT network, a stand-alone DTPA might be the easiest solution. This is typically an option for projects with an already settled CA or DTUA. It is strongly recommended to contact the PHI group before setting up such an agreement, in order to verify the selected DTPA covers all project needs.

Available combinations of legal agreements

Depending on the research project, it is crucial to define first the roles of project partners in order to decide for the architecture of legal agreements. To cover the respective needs of the project, different combinations of legal agreements are available on the webpage: Agreements building on the CA or full-fledged DTUA or DTPAs only. Please note that the templates available at the SPHN webpage https://sphn.ch/services/dtua/ provide a version using a single node or multiple nodes.

Approval and signature process

The first page of the legal agreement templates indicates the participating parties and specify the research partners' home institutions' information. The principal investigators (PI) do not need to be listed there. If, for example, the PI is affiliated with the University Hospital Basel, the following is provided: University Hospital Basel (USB), Spitalstrasse 21 / Petersgraben 4, CH - 4031 Basel.

Usually, the signature page includes the responsible local project leader and the duly authorized representative of the institution/hospital. The duly authorized representative designates the person, who is entitled to sign the institutional data sharing in accordance with signatures rules of the institution, such as the director of a university's research department. Some hospitals require additional persons signing, e.g. the CEO.

For SPHN projects, the signature is often collected by DocuSign, if project parties agree to use an unqualified electronic signature. Depending on the institutional process, a wet ink signature might be required. The responsible project leader has to verify with the legal department which process is appropriate.

Most importantly local project leader need to make sure they follow internal governance processes which typically require a review by their legal department and if applicable by a Data Access Committee.

Help and advice is available at the PHI Group: dcc@sib.swiss.