An ethical and legal framework for a responsible sharing and use of health data in multi-center research projects

Julia Maurer[1]*, Frederic Erard[2], Michael Müller-Brackenridge[1], Katrin Crameri[1#]

[1]SIB Swiss Institute of Bioinformatics, Personalized Health Informatics Group; [2]SIB Swiss Institute of Bioinformatics, Head Legal and Technology Transfer Office;
*presenting author, #corresponding author katrin.crameri@sib.swiss

The Swiss Personalized Health Network (SPHN) initiative aims to enable a nationwide use and sharing of data providing a secure infrastructure according to the FAIR (Findability, Accessibility, Interoperability, Reuse) principles. To ensure patient privacy and to promote data usage, responsible data-sharing policies must be agreed upon and adhered to in the Swiss research community.

Responsible health information exchange means that ethical and legal considerations must be taken into account. According to the SPHN ELSI Framework[1] and the SPHN Information Security Policy[2], the privacy of individuals providing data and the confidentiality of the personal information will be protected through technical and organizational measures. Research collaboration partners need a contractual framework and governance rules for data providing institutions to govern the general principles of collaboration and the conditions for sharing data with other parties. By promoting a responsible use of health data in biomedical research, SPHN has become the primary driving force for improving the nationwide ecosystem that meets regulatory requirements and addresses the conditions for making data available.

Protecting the privacy and integrity of patients

The importance of individual rights, privacy, data fairness and accountability has been illustrated in the published SPHN Ethical Framework[1,2] and implemented as part of the SPHN-funded research infrastructures.

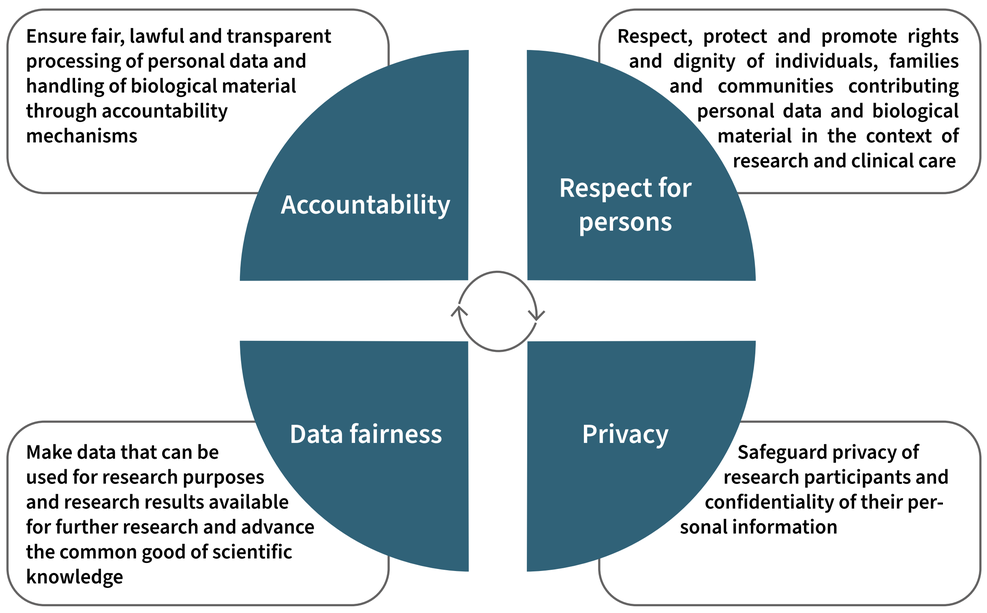

Figure 1: The SPHN Ethical Framework with its four principles.

An exemplary approach to protecting patient privacy in data sharing is the de-identification of personal health data. SPHN has produced hands-on recommendations based on a project-related, risk-based approach in accordance with Swiss law requirements[4] approach is divided into 3 phases and described in Figure 2.

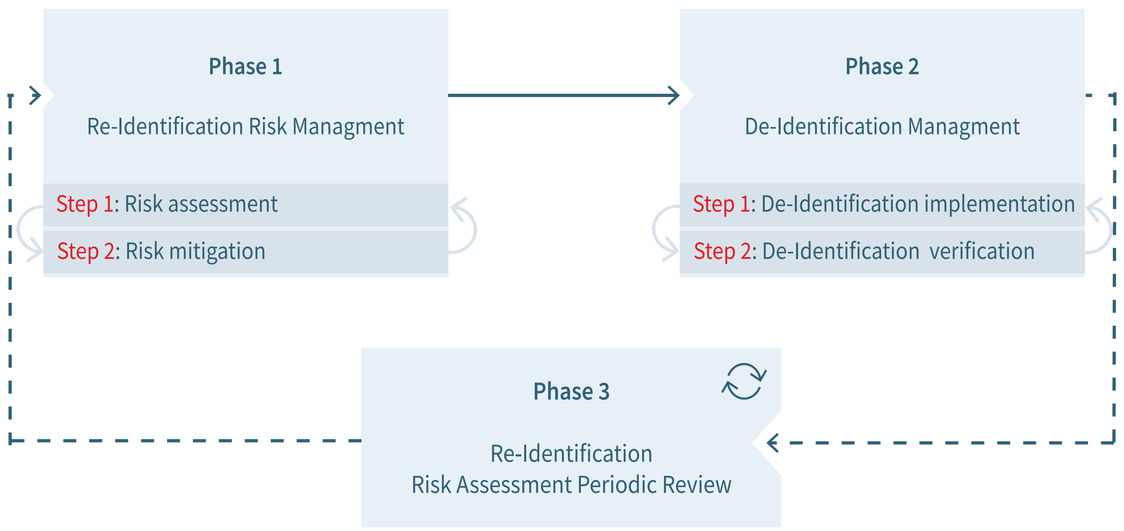

Figure 2: Phase 1 involves the re-identification risk management, assessing and mitigating patients' re-identification risk ; Phase 2 contains the implementation and verification of risk mitigation measures specified in phase 1; Phase 3 describes the periodic review of the risk assessment performed according to project specifications.

Regulating principles of collaboration and conditions of data sharing through legal agreements

Routine health data sharing requires data providing institutions to establish governance processes, and contractual frameworks need to be in place including the research collaboration partners. In SPHN, an overarching framework and legal agreement templates[5] to regulate general principles of collaboration and conditions under which data are disclosed to other parties has been set up. The legal agreement templates provided are built on a consolidated basis which was found with data providing and data using institutions for sharing sensitive data in multi-center projects. The approval workflow, which might be different for internal and external requests and thus concerns different decision bodies has to be well communicated by each institution.

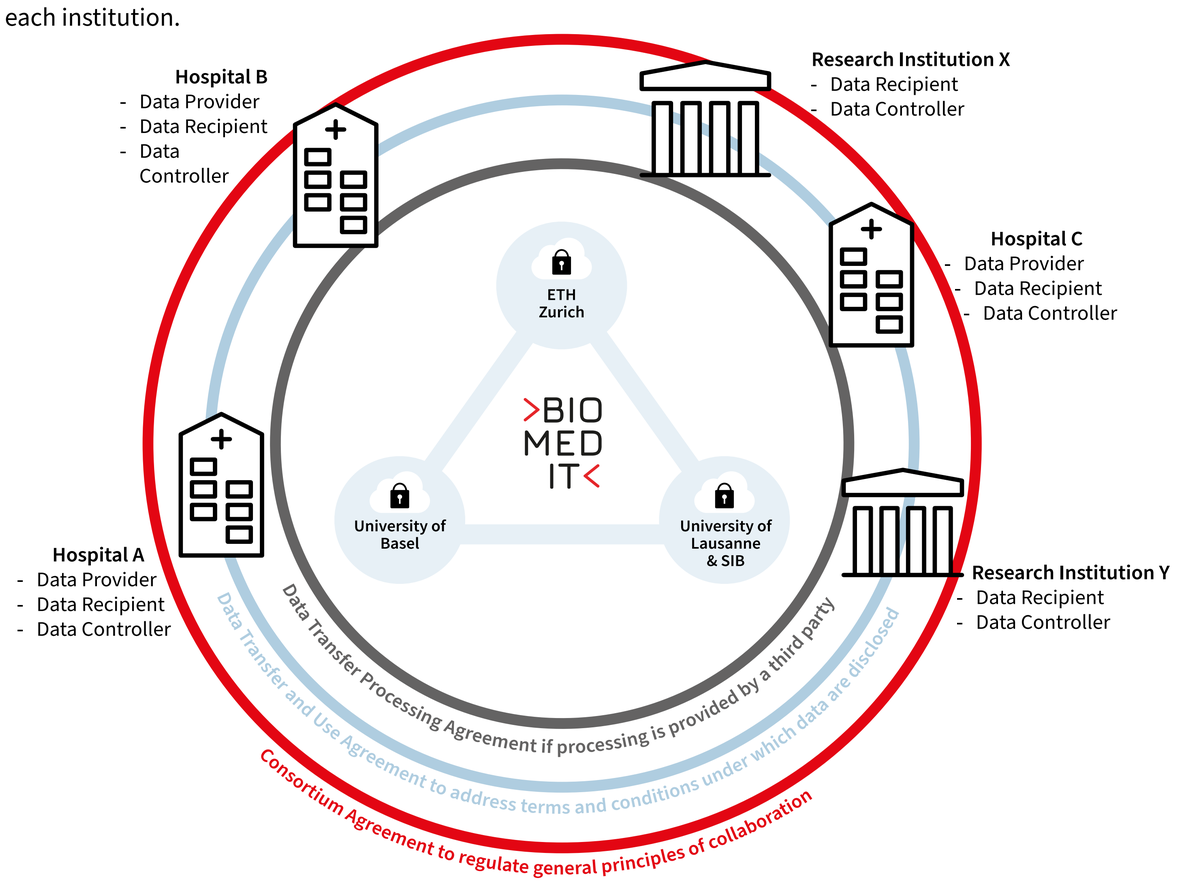

Figure 3: An overarching framework between the collaboration partners with the assigned roles of data provider, data recipient, data controller and data processor is essential to regulate the general principles of collaboration and the conditions for the data disclosure in the respective legal agreements.

References and further reading

[1]SPHN Ethical Framework

[2]SPHN ELSI Advisory Group

[3]SPHN Information Security Policy

[4]SPHN De-Identification Project

[5]SPHN Legal Agreement Templates

Secure IT platform for data processing and storage

The more systematically health data are used for research purposes, the more attention must be paid to ensuring that the used IT systems meet data protection and security requirements. To ensure information security, SPHN has implemented an Information Security Policy[3] that regulates the responsibilities and roles of the various parties. It provides for the management, monitoring and auditing of information security established within the BioMedIT network (see BioMedIT poster No.2).
Security measures are essential to protect sensitive personal data in accordance with the requirements of Swiss law.

In SPHN, data security measures were agreed upon by all university and university hospital partners to ensure 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 into the system is possible
- adequate organizational measures to protect data are in place.

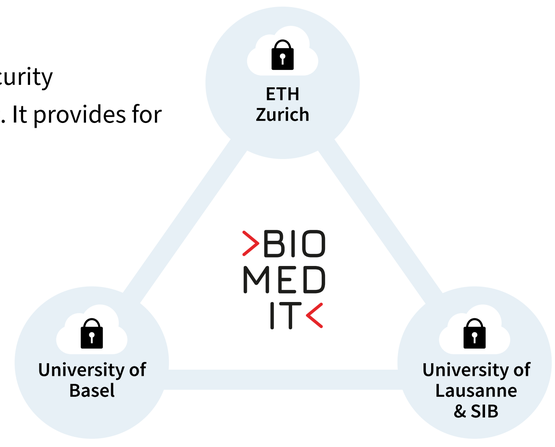

Figure 4: The BioMedIT network is a secure IT environment for the responsible storage and processing of health data as a service.

SPHN is funded by the Swiss State Secretariat for Education, Research and Innovation (SERI)

With thanks to the Swiss University Hospitals

University Hospital Basel · Hôpitaux Universitaires Genève · Inselspital Universitätsspital Bern Hopital universitaire de Berne Bern University Hospital · CHUV · USZ Universitäts Spital Zürich