Adherence Commitment by SPHN Participant

applicable to:

[details of participant to be identified here] (hereinafter the **Participant**)

Recitals

SPHN is a project facilitating the efficient use and transfer of Patient Data.

Participant wants to interact through SPHN with an entity making available Patient Data through SPHN.

As a condition, Participant declares to be bound by this document (the **Adherence Commitment**), including its Annexes:

Contents:

Details:

1. Scope

Data made available to Participant through SPHN shall be processed by Participant only as set out in this Instructions Document, or in its Annexes.

2. Definitions

For the purposes of this Adherence Commitment, capitalized terms shall mean the following:

2.1. “Personal Data”, “Special Categories of Data/Sensitive Data”, “Process/Processing”, “Controller”, “Processor”, and “Data Subject” shall have the same meaning as set out in the following legal grounds:

2.1.1. the Swiss Data Protection Act

2.1.2. the General Data Protection Regulation of the European Union (GDPR)

2.1.3. and the Directive 95/46/EC of 24 October 1995

as these legal grounds may apply.

2.2. "Authority” shall mean the competent data protection authority in the territory in which the Provider is established, and it can be more than one authority if more than one authority is competent.

2.3. "Participant" shall have the meaning given to it in on the first page of this Adherence Commitment.

2.4. “Provider” shall mean the university hospital or other player within SPHN to the extent it transfers Personal Data;

2.5. “Recipient” shall mean the Participant, other university hospital who agrees to receive from the Provider personal data for further processing in accordance with the terms of this Adherence Commitment;

2.6. “Adherence Commitment” shall mean this document, which is a free-standing document that does not incorporate commercial business terms established by the Participant and the Provider under separate commercial arrangements.

2.7. "Transferred Data" shall mean the Personal Data the Recipient will receive or has received from the Provider through SPHN.

3. Annexes

3.1. This Adherence Commitment has the following Annexes:

3.1.1. Annex A: Description of the Recipient.

3.1.2. Annex B: Project Description, including a description of the Transferred Data.

3.1.3. Annex C: Non Disclosure Obligation.

3.1.4. Annex D: Data Transfer Instructions.

3.1.5. Annex E: Data Processing Principles.

3.1.6. Annex F: Description of Technical Measures.

3.1.7. Annex G: Description of Organizational Measures.

3.1.8. Annex H: ELSI Requirements.

3.2. Annexes to this Adherence Commitment form an integral part of this Adherence Commitment and are binding upon Participant.

4. Minimum Requirements

4.1. The rules defined in this Adherence Commitment, and in its Annexes, are minimum requirements.

4.2. Own procedural rules of the Participant shall apply in addition if they go beyond this Adherence Commitment. However, if they do not meet the minimum requirements set out in this Adherence Commitment they are not relevant for systems on which Patient Data exchanged through SPHN are stored or processed; in such case, this Adherence Commitment shall apply.

5. Third Party Rights

Participant understands that Data Subjects can enforce rights related to their Personal Data against the Recipient or the Provider. Participant will serve such requests, and further adhere to the Communication Guidelines set out in Clause 6.

6. Communication Guidelines

6.1. Participant commits to informing the Provider about each request it receives under Clause 5.

6.2. Participant commits to respond to requests of Data Subjects swiftly, by submitting standard responses to requests about (i) correction of data; (ii) deletion of data; (iii) a clarifying notice to be added along with some data; (iv) withdrawal of consent; (v) data portability / release of a copy (release of a data set) if such requests relate to the Transferred Data. The Standard responses are meant to be first responses: (a) informing the requesting Data Subject about the process that applies and (b) informing the requesting Data Subject about the timeline within which it can expect to see its request implemented. [Reference to standard text here: TBD]

6.3. Participant commits to take all measures available to it in order to avoid data breaches. If nevertheless a breach should occur, Participant shall inform about occurred data breaches as follows: [standard text to be defined in order to make sure the Provider is not in the focus, to make sure the process required by law is met, and to make sure to comply with transparency requirements set out in the law.]

6.4. After having released the standard notices described in Clauses 6.1 and 6.2 (as applicable) Participant will immediately align with the Provider in order to jointly determine the lead role for further dealing with the request. The Provider and the Recipient shall agree on the lead role, and further communication routines they will adhere to until the request of the Data Subject has been served in full.

7. Education of Users

Participant accepts that it must educate its personnel on an ongoing basis. [Details could be added in Annexes, e.g. in Annex F: Processing Instructions].

8. Indemnification

8.1. The parties will indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of this Adherence Commitment.

8.2. Indemnification hereunder is contingent upon (a) the party(ies) to be indemnified (the "indemnified party(ies)") promptly notifying the other party(ies) (the "indemnifying party(ies)") of a claim, (b) the indemnifying party(ies) having sole control of the defence and settlement of any such claim, and (c) the indemnified party(ies) providing reasonable cooperation and assistance to the indemnifying party(ies) in defence of such claim.

9. Confidentiality

Participant agrees that the Personal Data it requests may contain confidential business information which it will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency. Participant declares to be bound by the Non Disclosure Obligations set out in Annex D to this Adherence Commitment.

10. Return and destruction of personal data

10.1. Upon finishing the processing of Transferred Data, Participant must return all Personal Data and all copies of the Personal Data to the Provider forthwith or, at the Provider's choice, destroy all copies of the same and certify to the Provider that it has done so, unless the Recipient is prevented by applicable law from destroying or returning all or part of such data, in which event the data will be kept confidential and will no longer be actively processed for any purpose.

10.2. The Recipient agrees that, if so requested by the Provider, it will allow the Provider, or an inspection agent selected by the Provider and not reasonably objected to by the Recipient, access to its establishment, with reasonable advance notice and during business hours, to verify that Recipient has complied with Clause 10.1.

11. Applicable Law

Participant exclusively submit to the substantive Swiss Law, and exclude the conflict of law rules of the Swiss Private International Law Act (SPILA).

12. Dispute Settlement

Participant exclusively submits to the jurisdiction of the ordinary civil courts at the place of business of the Provider. Each dispute among the Provider and the Recipient shall exclusively be resolved by such civil court. [Note: This rules should be analyzed in more detail by each UH in order to make sure that civil courts would have jurisdiction.]

PARTICIPANT

____
(Place, Date)

____
Signatory 1

____
Signatory 2

Annex A Information about Recipient

Recitals

This document is re an Annex to the overall SPHN Adherence Commitment each participant to SPHN must adhere to.

Recipient Name	
Recipient Address	
Recipient Program Lead / Project Lead	
Recipient Key Personnel for Project	
Recipient Contact - **Email:** - **Phone:**	
Recipient Data Protection Officer	
Project Ethical Approval	

Annex B Project Description and Description of Transfer

Recitals

This document is an Annex to the SPHN Adherence Commitment each participant to SPHN must adhere to.

It describes the data-related core aspects of the Project for which the Recipient requires access to data through SPHN:

1 Description of Recipient's Research Project

[Recipient to describe the Research Project for which it intends to receive Patient Data.]
[Recipient to describe the Objectives of the Research Project it wishes to receive Patient Data for.]
[Recipient to refer to the approval obtained by the Ethics Committee.]
[This Annex must be updated whenever the Research Project is amended, or if a new Research Project has been submitted and for which, after approval of the Ethics Committee, a data request through SPHN has been requested.]

2 Purposes of the Transfer(s)

The transfer is made for the following purposes:

[Recipient to describe the Purpose of the intended transfer from Provider to Recipient. Usually, the description under item 1 would suffice, in such event note state "see description of the Research Project". If additional purposes should be covered this should be noted here.]

3 Intended Processing

[Recipient to describe the intended methods of processing; "business" processes should be described, e.g. by way of a diagram.]

4 Content of the Data Set Recipient wishes to Receive

[Recipient to describe the Patient Data it wishes to receive:]

[- nature of Personal Data]

[- categories of Personal Data]

[- expected origin of Personal Data]

5 Sensitive Data

The personal data transferred concern the following categories of sensitive data:

[Recipient to describe which to what extent the Transferred Data are Sensitive Data or belong to a "Special Category of Data" in the meaning of the GDPR.]

6 Data subjects

The Transferred Data concern the following categories of Data Subjects:

[Recipient to describe the Patient Data as required.]

7 Categories of data

[Recipient to describe which categories of data are in the Transferred Data.]

8 Intended Recipients of data

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

[Recipient to describe which recipients might access the Transferred Data.]

9 Users of the Personal Data

[Recipient to describe which categories of users will have access to the Personal Data in question]

[Purposes for which users will have access to the Personal Data in question]

[Justification for users to access the Personal Data]

10 Data Access Concept

[Recipient to describe the roles to whom access is being granted]

[Recipient to describe the process how access to data will be granted]

[Recipient to describe the data access matrix]

Data Fields	Recipient						Third Parties					
	OE	OE	OE	…	…	…	OE	OE	…	…	…	…
I. Stammdaten												
Name(n)	A	A	B	…	…	…	A	…	…	…	…	…
Vorname(n)	A	A	B	…	…	…	A	…	…	…	…	…
Geburtsdatum		A	A	…	…	…	A	…	…	…	…	…
Staatsangehörigkeit		A	A	…	…	…	B	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…	…

II. Health Related Data												
…	B	B	B	…	…	…	A	…	…	…	…	…
…	B	B	B	…	…	…		…	…	…	…	…
…	A	B	B	…	…	…	B	…	…	…	…	…
…												
III. Titel X												
…												
…												
…												

Access Levels
A = Read Access
B = Read/Write Access
empty = no access
other

Organizational Entities (OE)

OE I:	e.g. Researchers of the respective OE
OE II:	a.g. Administrators of the respective OE
OE III:	…
…	

11 Data Communication and Interfaces

[Recipient to describe the intended disclosures, if any, whether by way of direct communication or by way of technical establishment, such as interfaces. Recipient must not disclose Personal Data, including Patient Data, it has received through SPHN without receiving a prior waiver of confidentiality etc. from the Provider]

[If by way of interfaces, additional details should be added, e.g.: who will receive the Personal Data? For which purposes? Which categories of Personal Data? Who would initiate data transfer?]

12 Anonymization and Pseudonymization

[Recipient to describe mechanisms to anonymize and pseudonymize Personal Data it has received through SPHN, if possible. If not possible, it should be described why not.]

13 Storage, Archiving, Deletion

[Recipient to describe mechanisms to store, archive and delete Personal Data received through SPHN. Retention Periods should be identified.]

14 Control Mechanisms

[Recipient to describe control mechanisms to ensure compliance with the obligations it has under the Adherence Commitment]

15 Data Protection Registration Information of Recipient

The Recipient has submitted the following registrations with a competent Data Protection Authority:

[Recipient to describe to what extent it has submitted a data protection related or ethically required notification to a competent authority or to what extent it expects submitting such notification in anticipation of the project. Recipient should identify whether the processing will be notified to Federal Data Protection and Information Commissioner.]

16 Responsible Managers of Recipient

[Recipient to describe who will be responsible of the processing it intends to perform with respect to the Personal Data it wishes to receive:]

[- Responsible Manager]

[- Project Lead]

[- Internal Application Responsibles]

[- Internal Responsibles for Network Operation, Database Operation, etc., and third parties used to perform related activities]

[- Internal Data Protection Officer]

[- Alternatively, Recipient can make reference to an existing Information Security and Data Protection Concept]

17 Contact Points for data protection enquiries

The Recipient's Contact Points for Data Protection Enquiries is as follows:

[Recipient to describe its competent contact points who can communicate on the items discussed in this Annex]

18 Process to respond to requests of Data Subjects / Patients

[Recipient to describe the methods of how requests of Data Subjects / Patients shall be dealt with. The responsible managers dealing with such requests should be identified.]

Annex C Non Disclosure Obligations of Recipient

Recitals

This document is an Annex to the SPHN Adherence Commitment each participant to SPHN must adhere to.

It describes the data-related core aspects of the Project for which the Recipient requires access to data through SPHN:

1. Recipient hereby undertakes that it shall, and procure that its personnel shall, in respect of any Confidential Information disclosed by a Disclosing Party:

   1.1. use such Confidential Information only for the purposes indicated by the Disclosing Party the "Permitted Purpose"), and not to use such disclosed Confidential Information for any other purpose; and

   1.2. maintain strictly confidential all Confidential Information; and

   1.3. comply with such other instructions as the Disclosing Party may give to the Recipient with respect to the Disclosing Party's Confidential Information.

2. Recipient shall not give or permit access to any Confidential Information to any of its Personnel other than those who reasonably require to see and use it for the Permitted Purpose. The Recipient shall inform each of its Personnel to whom any Confidential Information (or access to it) needs to be given that such Confidential Information is confidential.

3. Subject to mandatory applicable law, and unless the Parties agree otherwise in writing, on termination or completion of the Permitted Purpose (or at any time before on request from a Disclosing Party) the Recipient shall:

   3.1. deliver up to the Disclosing Party; and/or

   3.2. destroy and expunge permanently from its systems (to the extent reasonably feasible), all documents, materials and other media in its or any of its Personnel's control that contain, bear or incorporate any part of any Confidential Information, and the Recipient shall provide to the Disclosing Party on request a written confirmation that all such documents, materials and other media have been so delivered, destroyed or expunged.

4. The foregoing provisions of this section 3 shall not apply to any Confidential Information which:

   4.1. at the date of this Agreement or any time thereafter becomes available to the public other than by breach of this Agreement; or

   4.2. was rightfully received from a third party not in breach of any obligation of confidentiality; or

   4.3. was known, or independently developed, by the Recipient without reference to the Confidential Information of the Disclosing Party; or

   4.4. was produced on a non-confidential basis in compliance with applicable law or court order.

5. Recipient shall use its reasonable efforts to ensure that appropriate internal confidentiality and information security procedures are in place and are used to protect any Confidential Information,

where necessary, within its organization and that such procedures are established and maintained in accordance with up-to-date professional and/or industry standards.

Annex D Data Transfer Instructions

Recitals

These Data Transfer Instructions are an Annex to the overall SPHN Instructions Document each participant to SPHN must adhere to.

Data Transfer Instructions:

1. Obligations of Providers

Recipient understands that it is expected to adhere to this document on the basis of the Provider's undertaking that, and that it has the right to request the Provider to confirm the following in a separate agreement between the Recipient and the Provider:

1.1. The Personal Data have been collected by the Provider, processed and transferred to Recipient in accordance with the laws applicable to the Provider.

1.2. The Provider will respond to enquiries from data subjects and the authority concerning processing of the personal data by the Recipient, unless the Provider and the Recipient have, with regard to the Transferred Data, agreed that the Recipient will so respond.

1.3. The Provider may still respond to the extent reasonably possible and with the information reasonably available to the Provider if the Recipient is unwilling or unable to respond.

2. Obligations of Recipients

Recipient undertakes that:

2.1. It will have in place appropriate technical and organizational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

2.2. Subject to Clause 2.3, the following shall apply: Recipient will have in place procedures so that any third party it authorizes to have access to the Personal Data, including processors and employees, will respect and maintain the confidentiality and security of the Personal Data. Any person acting under the authority of the Recipient, including a data processor or employee, shall be obliged to process the Personal Data only upon instruction from the Recipient. This provision does not apply to persons authorized or required by law or regulation to have access to the personal data.

2.3. Notwithstanding the foregoing, Recipient shall be bound by the Non Disclosure obligations set out in [Annex C].

2.4. Recipient will process the Personal Data for purposes described in [Annex B], and has the legal authority to fulfil the undertakings set out in these Data Transfer Instructions.

2.5. Recipient will identify to the Provider a contact point within its organization authorized to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the Provider, the data subject and the authority concerning all such enquiries within a reasonable time. Such contact point will further be described in [Annex B].

2.6. At the request of the Provider, it will provide the Provider with evidence of financial resources sufficient to fulfil its responsibilities under the Adherence Commitment, and its Annexes (which may include insurance coverage).

2.7. Upon reasonable request of the Provider, Recipient will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the Provider (or any independent or impartial inspection agents or auditors, selected by the Provider and not reasonably objected to by the Recipient) to ascertain compliance with the undertakings in these Data Transfer Instructions, with reasonable notice and during regular business hours.

2.8. It will process the personal data in accordance with the data protection laws of Switzerland [TBD, if foreign nexus: "the country in which the Provider is established or the country whose laws apply"], and with the data processing principles set forth in [Annex E].

2.9. It will not disclose or transfer the Personal Data to a third party data controller unless it notifies the Provider in advance about the intended transfer so that the Provider can procure consent declarations from the Data Subjects. Recipient will only communicate Personal Data to third parties after Data Subjects have given their unambiguous consent to the onward transfer. If the Provider is unable to procure such consent it can prohibit the onward transfer. For the avoidance of doubt, if Recipient intends to use processors for the purposes of organizing its IT infrastructures this shall not be an event of onward transfer (provided Recipient has established sufficient control over the processor).

3. Description of the transfer

The details of the transfer and of the personal data are specified in [Annex B].

Annex E Processing Instructions

Recitals

These Processing Instructions are an Annex to the overall SPHN Instructions Document each participant to SPHN must adhere to.

Data Processing Instructions:

1. Obligations of Recipients

Any Recipient undertakes to

1.1. Set up adequate documentation to describe the mode of operation and the architecture of the IT systems it has in place.

1.2. To apply at least the standards set out in Annex F (Technical Measures) and Annex G (Organizational Measures).

2. Data Processing Principles

2.1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorized by the data subject.

2.2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The Personal Data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

2.3. Transparency: Data Subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the Provider.

2.4. Security and confidentiality: Technical and organizational security measures must be taken that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the Recipient, including a processor, must not process the data except upon instruction from the Recipient.

2.5. Rights of access, rectification, deletion and objection:

2.5.1. Data Subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under no law that applies (neither the country of the Provider nor the country of the Recipient).

2.5.2. [TBD / possibly to be amended]: Provided that the Authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the Recipient or other organizations dealing with the Recipient and such interests are not overridden by the interests for fundamental rights and freedoms of the Data Subject.

2.5.3. The sources of the Personal Data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data Subjects must be able to have the Personal Data about them rectified, amended, or deleted where it is inaccurate or processed against these principles.

2.5.4. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion.

2.5.5. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort.

2.5.6. A Data Subject must also be able to object to the processing of the Personal Data relating to him or her if there are compelling legitimate grounds relating to his particular situation.

2.5.7. The burden of proof for any refusal rests on the Recipient, and the Data Subject may always challenge a refusal before the Authority.

2.6. Sensitive data: The Recipient shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under applicable data protection law.

2.7. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the Recipient which produces legal effects concerning a Data Subject or significantly affects a Data Subject and which is based solely on automated processing of Personal Data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The Recipient shall not make any automated decisions concerning Data Subjects, except when:

2.7.1. [omitted]

2.7.2. the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the Recipient or otherwise to submit a statement or objection to the Recipient;

or where otherwise provided by applicable law.

Annex F Description of Technical Measures

Recitals

This Document is an Annex to the overall SPHN Instructions Document.

When submitting an application to participate in the SPHN, Participant must hand in material to evidence that it has sufficient technical measures in place to protect the Personal Data which it wishes to receive.

The technical measures must be described. Mere references to certifications (e.g. ISO 27001) are not sufficient.

The [DCC] will review this document before the Participant will be admitted to SPHN.

The Participant's technical measures to protect the data it will receive are / will be:

[to be filled]

Annex G Description of Organizational Measures

Recitals

This Document is an Annex to the overall SPHN Instructions Document.

When submitting an application to participate in the SPHN, Participant must hand in material to evidence that it has sufficient organizational measures in place to protect the Personal Data which it wishes to receive.

The organizational measures must be described. Mere references to certifications (e.g. ISO 27001) are not sufficient.

The [DCC] will review this document before the Participant will be admitted to SPHN.

The Participant's organizational measures to protect the data it will receive are / will be:

[to be filled]

Ethical Framework for Responsible Data Processing in the Swiss Personalized Health Network

ELSI Advisory Group (12.06.2017)

I. Scope and purpose

The Ethical Legal and Social Implications advisory group (ELSIag) of the SPHN was mandated to produce ethical guidance in relation to personal data processing within the SPHN, with particular emphasis on guidance for data sharing. To this aim, the ELSIag has produced an ethical framework (henceforth, the Framework) for the responsible processing of personal data in the SPHN (henceforth, the Network). The methodology that led to this Framework is described in a separate document. The Framework provides ethical guidance to the partners of the Network as to the collection, storage, analysis and sharing of personal data for research purposes. It is based on a systematic analysis of international guidelines in this area, which provide comprehensive coverage if additional issues, but it is focussed on the specific needs of the SPHN in its early phase of development. Compliance with national laws and with this framework are requirements for participation in the SPHN funding schemes and activities.

The purpose of the Framework is to ensure that the scientific activities in relation to personal data that are conducted in the context of the SPHN meet adequate standards of ethical sustainability, promote the rights, interests and well-being of research participants, ensure the efficient production of valuable scientific knowledge, and generate public trust around the activities of the Network.

The Framework refers to all data types that can be usefully employed in the context of health research. This includes data that were not originally collected for research purposes (such as clinical data), as well as data that are not conventionally associated with the practice of medical research (such as geolocalization data, social media content, data from commercial portable sensors and the like).

The Framework is built on four general principles: scientific progress, respect for persons, privacy and accountability. Each principle is followed by a set of specific guidelines intended to assist SPHN partners to abide by the principles.

In addition, this document contains definitions of the most relevant terms employed in the Framework and a checklist that corresponds to the guidelines.

Disclaimer:

- The ELSIag and SPHN are not responsible for oversight and compliance with this framework.
- This document will be periodically reviewed and will be amended in consultation with other governing bodies of the SPHN. It will also be supplemented with additional policies according to the needs of the SPHN network.

II. Definitions

Further research use = all research uses beyond the scope of initial collection (e.g. data collected in the context of one research project and still usable for other studies unrelated to the original one; clinical data initially collected for diagnostic purposes).

Participating institution = institutions that are active in SPHN but do not necessarily receive funding (i.e. private entities or foreign research groups).

Research participants = individuals who contribute data to SPHN research, including, both individuals currently or previously enrolled in a research study and patients whose data are used in a SPHN-related study; and more generally the natural and legal persons whose data are being processed.

Personal data = all information relating to an identified or identifiable person.

Secondary findings = all medically-relevant information that can be derived from data analyses beyond the initial scope of collection.

Encoded = data linked to a specific person via a code.

Anonymized data = data that cannot possibly be linked back to an identifiable individual without disproportionate effort.

General consent = informed consent of a research participant to unspecified further research uses of her personal data. It is synonymous to *broad consent*.

Data processing = any operation with personal data, irrespective of the means and the procedure employed, and in particular the collection, storage, use, sharing, revision, disclosure, archiving or destruction of data.

Informational self-determination = the right to control one's own personal information, i.e. the right to determine which information will be disclosed when, to whom and for what purpose.

III. Ethical principles and guidelines for responsible data processing in the Swiss Personalized Health Network (SPHN)

We have identified four ethical principles that should guide the conduct of researchers and the activities of institutions that participate in the SPHN when processing health related personal data. In particular, this documents aims to guide the sharing of such data within the SPHN.

1. Respect for persons

The rights and dignity of individuals, families and communities contributing health data in the context of research and clinical care, as well as other types of data that can be useful for biomedical research must be respected, protected and promoted.

Individuals have universal human rights, enjoy intrinsic moral worth and have a fundamental entitlement to act as autonomous persons. This includes a right to informational self-determination, that is, the right to control the terms under which personal data are processed. These fundamental rights shall always take precedence over the interests of scientific knowledge and shall be respected and protected by anyone who processes personal data for any purpose and at any time.

Enrollment in a research study and collection and use of personal data shall always be informed and fully voluntary acts. Withdrawal from a research study and, unless technically impossible, removal of personal data from a research database shall never lead to negative consequences for research participants.

Individuals, families, and communities who agree to participate in a scientific study and provide personal data for research purposes, do so without an expectation of direct benefit and mostly out of altruistic motivations or inspired by moral ideals of solidarity. Nevertheless, they have the right to receive at least clinically actionable information that may result from the analysis of their data.

Guidelines

a) Non-genetic health-related data, whether they are encoded or not, shall be made available for further research use by participating institutions, provided at least general consent has been obtained.

b) All anonymized genetic data shall be made available for further research use by participating institutions provided research participants have agreed to anonymization, have been informed about the intention to use such anonymized data for research and have not dissented to it.

c) All encoded genetic data shall be made available for further research use by participating institutions, provided at least general consent has been obtained.

- i) A general consent template is available in Annex 1 and is recommended for use.

d) All personally identifying genetic data shall be made available for further research use by participating institutions if individuals have provided prior informed consent for the specific use in question.

e) Health related personal data for which informed consent is not available, nor possible to obtain can be made available for further research use by participating institutions provided an authorization is obtained by the competent cantonal ethics committee – following the conditions set forth by the law (HRA art. 34).

f) Participating institutions should have mechanisms in place that ensure revocation of consent is swiftly acted upon across the network of data users.

g) Clinically actionable findings should be communicated to research participants through caregivers, unless participants have objected to being recontacted during informed consent procedures.

h) Criteria for determining clinically actionable findings will be elaborated by the ELSIag at a later stage and shall guide decisions about recontacting research participants.

i) Participating institutions should have standardized procedures regarding the communication of clinically actionable findings and of clinically relevant results in case research participants request disclosure of such results.

2. Privacy

Privacy and confidentiality must be safeguarded.

All persons possess a fundamental interest in not having personal information accessed or distributed without their authorization, or used in inappropriate illicit or harmful ways. For this reason, the collection, use and sharing of personal data for research purposes shall only take place under the condition that individuals' right to privacy is respected.

Appropriate measures for the protection of privacy and against the risk of privacy breaches must be taken, for instance, by implementing security controls such as techniques of data de-identification, advanced data anonymization and cryptography, and by preventing access to personal data beyond the specific research needs. In the context of scientific research, confidentiality fosters trust in the activity of researchers and institutions that collect, store, use, distribute or access personal data, both patients' data as well as data of healthy individuals.

All necessary data security measures should be adopted to protect personal data form unauthorized access, intentional or unintentional alteration, damage, loss and misuse.

Guidelines

a) The institutions participating in the SPHN shall abide by data security measures as prescribed by the Data Coordination Center.

b) Participating institutions should abide by professional standards of confidentiality with respect to personal data as stated in relevant professional codes of conduct.

c) Participating institutions are responsible for encoding and anonymization of personal data, as well as for reidentification procedures (e.g. in case of return of clinically actionable findings). Relevant mechanisms will be articulated by the Data Coordination Center.

d) The personnel employed in data-related activities shall be appropriately trained on the technical, legal and ethical requirements with regard to data protection and the management of personal data.

3. Data Fairness

Data that can be used for research purposes and research results should be made available for further research use to advance the common good of scientific knowledge.

The availability of data is a major determinant of scientific progress. Data can greatly contribute to the advancement of biomedicine and to the improvement of healthcare. The possibility of using data collected and generated in the context of both research and clinical care, as well as other types of data that can be useful for biomedical research is in the interest of the scientific community, individuals and society. These data often have value well beyond their primary purpose of collection and use, provided other researchers are able to access them for further analysis. Data and results should thus be shared among researchers or anyway be made available for further research or clinical use.

Moreover, certain types of data – like reference genetic sequences, for example – are indispensable assets for progress in specific scientific domains and should thus be considered as community resources and should be made available as soon as possible.

The researchers and institutions originally involved in the creation of a given dataset shall be given full recognition for their work. Researchers and institutions that generated data though public funding shall not have exclusive access rights to these data sources.

Guidelines

a) The SPHN is committed to maximizing data availability for research use. Therefore, it requires participating institutions to make their relevant data accessible to the network partners for further research use.

b) Access to data should be made possible in a timely manner. In case of delayed data releases, a justification should be provided to the SPHN Management Office.

c) Within SPHN, partners should make data accessible without financial profit, and cannot grant exclusive data access rights to any other party.

d) Costs associated with making data accessible can give rise to compensation either in kind or through an appropriate data access fee. Such costs should be included in the requested funding.

e) Data users should give proper recognition and credit to those who provided the data.

   i) Norms for authorship attribution are specified in the Swiss Academies of Arts and Sciences' recommendations for authorship in scientific publications[1], and should be followed.

   ii) Issues of intellectual property attribution will be dealt with at the institutional level by each SPHN partner.

f) Data shared within the SPHN infrastructure shall be accompanied by a description of the procedures used to generate them, as well as adequate metadata. Moreover, shared data should adhere to formats and standards defined by the interoperability working group led by the Data Coordination Center to ensure optimal interoperability.

g) SPHN partners should plan in advance how to disseminate research results to the wider public.

[1] Scientific Integrity Committee of Swiss Academies of Arts And Sciences, Christian W. Hess, Christian Brcienti, Tony Kaiser, Alex Mauron, Walter Wahli, Uwe Justus Wenzel, and Michelle SalathJ. 2015. stus Wenzel, and Michelle Salathalathle SalathSalath and Mmendations.at*Swiss Medical Weekly* 145: w14108. doi:10.4414/smw.2015.14108.

4. Accountability

Accountability mechanism should ensure fair, lawful and transparent data processing.

The existence of adequate governance structures is a prerequisite for the use of personal data in the context of scientific research.

Accountability requires that organizations processing personal data for research purposes can be held responsible for the consequences their activities may have on both research participants and society as a whole. This requirement fulfils basic duties of fairness.

Compliance with existing legal norms and regulations regarding the use of personal data for research purposes is the baseline of accountability. However, whenever appropriate, additional measures should be adopted in order to provide better protection to the legitimate interests of research participants.

Procedures and mechanisms adopted by research organizations to govern their data processing activities should be open to scrutiny. In particular, research participants have a right to access information regarding how an organization processes their data including the conditions under which it grants access to other data users. These basic principles of transparency are constitutive elements of accountability.

Robust accountability mechanisms promote public trust and foster a climate of mutual respect and reciprocity between research institutions, research participants and the general public.

Guidelines

a) Given the implications that the use of personal data may have for research participants, responsibilities for the use of such data should be clearly identifiable.

b) The governance structure of the participating institution must be transparent and auditable.

c) Procedures for authorization of data access requests within the participating institutions should be lean, standardized and transparent.

d) Requests by third parties for access to data produced through SPHN-funding should undergo ethical assessment.

e) Appropriate functions such as monitoring, performance evaluation and periodic auditing of data security measures shall be undertaken by each participating institution. Results from these activities should periodically be transmitted to the SPHN Data Coordination Center.

f) The participating institutions are responsible for legal compliance with human research and data protection laws.

g) The personnel employed in data-related activities shall be appropriately trained on the technical, legal and ethical requirements with regard to data protection and the management of personal data.