# DATA TRANSFER AND USE AGREEMENT

for the SPHN Infrastructure Project
*SwissPK$^{cdw}$: Optimizing pediatric dosage regimens based on a clinical data warehouse*

This agreement (hereinafter referred to as the "Agreement") is made and entered into by and between:

**University Children's Hospital Basel**, Spitalstrasse 22, CH - 4056 Basel

and

**University Children's Hospital Zurich**, Steinwiesstrasse 75, CH - 8032 Zurich

and

**University of Basel**, Hebelstrasse 20, CH - 4031 Basel

and

**ETH Zurich**, Hauptgebäude, Rämistrasse 101, CH - 8092 Zurich

Hereinafter jointly referred to as the "PARTIES" and individually as a "PARTY";

**WHEREAS**

a) The PARTIES have been granted support by SPHN for their joint research Infrastructure Development Project number 2018DEV21 "*SwissPK$^{cdw}$: Optimizing pediatric dosage regimens based on a clinical data warehouse*" (hereinafter referred to as the "RESEARCH"). A PARTY providing DATA to another PARTY under this Agreement shall be considered a PROVIDER for the purposes of this Agreement. A PARTY receiving DATA from another PARTY under this Agreement shall be considered a RECIPIENT for the purposes of this Agreement.

b) The PROVIDER is the controller of data (hereinafter referred to as the "DATA"), as set forth in **Annex I** of this Agreement;

c) The RECIPIENT wishes to conduct the RESEARCH, as set forth in **Annex II** of this Agreement, with the DATA made available by the PROVIDER. The PROVIDER is willing to provide such DATA to the RECIPIENT under the terms and conditions as follows hereafter.

**I. Definitions**

Unless defined below, terms shall have the meaning described in the applicable law; in case there is no definition in the law, the SPHN Glossary (https://sphn.ch/wp-content/uploads/2019/11/Glossary_20180530_SPHN-1.pdf) definition shall apply.

For the purpose of this Agreement, capitalized terms, whether used in singular or plural form, shall have the following meaning:

1. **BACKGROUND INTELLECTUAL PROPERTY (BACKGROUND IP)**: shall have the meaning set forth in Section V below.

2. **CODED DATA** or **DATA IN CODED FORM**: means the data linked to a specific person via a code.

3. **CONFIDENTIAL INFORMATION**: means any data, documents or other material (in any form) that is identified as confidential in writing at the time it is disclosed hereunder by a PARTY to its counterpart.

4. **DATA**: means all the data, including the metadata, being transferred (or if not transferred, the data given access to) under this Agreement, as set forth in **Annex I** of this Agreement.

5. **DATA SUBJECT**: means the natural person whose data is processed.

6. **EFFECTIVE DATE**: means 01.11.2019.

7. **FOREGROUND INTELLECTUAL PROPERTY (FOREGROUND IP)**: shall have the meaning set forth in Section V below.

8. **INTELLECTUAL PROPERTY RIGHTS:** means all intellectual property rights throughout the world, whether existing under statute, at common law or equity, registered or unregistered, now or hereafter in force or recognized, including trade secrets and know-how.

9. **PROVIDER'S PROJECT LEADER:** means the PROVIDER's person who takes responsibility for the project as described in the Ordinance on Human Research (HRO).

10. **RECIPIENT'S PROJECT LEADER:** means the RECIPIENT's person who takes responsibility for the project as described in the HRO.

11. **RESEARCH**: means the research project as set forth in **Annex II** of this Agreement, as approved by the Ethics Committee, and for which the DATA will be used;

12. **RESULTS**: means without limitation any output of the RESEARCH such as invention, data, software, algorithms, knowledge, know-how or information that is generated in the RESEARCH, whatever its form or nature, whether or not it can be protected, as well as any rights attached to it, including INTELLECTUAL PROPERTY RIGHTS.

## II. DATA Provision

1. **Form.** The DATA shall be provided to the RECIPIENT by the PROVIDER in a CODED FORM and in a format to be agreed upon by the PARTIES as per **Annex III.** The RECIPIENT shall not have the key.

2. **PROVIDER's Warranties about DATA Provision** – The PROVIDER warrants that it is entitled to supply the DATA and that all necessary consents and/or authorizations for the transfer and/or use of the DATA to/by the RECIPIENT have been obtained.

3. **No PROVIDER's Warranties about DATA.** It is expressly understood that the PROVIDER does not warrant or guarantee that the DATA will be accurate, complete, or useful for any particular purpose.

4. **No PROVIDER's Warranties about Third Parties' INTELLECTUAL PROPERTY RIGHTS.** The PROVIDER offers no warranty that the use of DATA and/or CONFIDENTIAL INFORMATION will not infringe or violate any patent or other proprietary rights of any third party.

## III. DATA Processing

1. **Purpose**. The RECIPIENT and the RECIPIENT'S PROJECT LEADER agree that the DATA: (a) is to be used only for the academic purposes as described in the plan on the RESEARCH; (b) may not itself be commercialized and (c) shall not be transferred to or accessed by any third party, for any purposes whatsoever, without the prior written agreement of the PROVIDER and in compliance with the informed consent of the DATA SUBJECT.

2. **Ownership.** The DATA provided is and remains the property of the DATA SUBJECT. The CONFIDENTIAL INFORMATION provided is and remains the property of the PROVIDER.

3. **Security**. The RECIPIENT shall process the DATA in a manner that ensures appropriate security of the DATA, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality'), as further described in **Annex IV**, as well as in the "*Ethical Framework for Responsible Data Processing in Personalized Health Research*" and in the *"SPHN Information Security Policy*", as both updated occasionally, accessible at:

   https://sphn.ch/wp-ontent/uploads/2019/11/Ethical_Framework_20180507_SPHN.pdf
   https://sphn.ch/wp-content/uploads/2020/01/sphn_information_security_policy_v1.pdf

The RECIPIENT agrees to immediately report (i) any actual or suspected data protection breach, including a breach against applicable data protection regulation, data protection section of this Agreement, (ii) any actual or suspected impairment or inadequacy of the RECIPIENT in fulfilling data protection section of this Agreement, and (iii) any application to receive or any actual access to data by an authority, unless such reporting is not admissible under statutory provisions for important reasons of public interest.

The RECIPIENT shall have in place procedures so that any person it authorizes to have access to the DATA, including the RECIPIENT'S PROJECT LEADER and their authorized users, will respect and maintain the confidentiality and security of the DATA. Any person acting under the authority of the RECIPIENT shall be obligated to process the DATA only on instructions from the RECIPIENT'S PROJECT LEADER.

In case the RECIPIENT'S PROJECT LEADER or the PROVIDER'S PROJECT LEADER is replaced, the other PARTY must be notified without delay. The RECIPIENT and the RECIPIENT's authorized users shall not (i) provide any output or RESULTS of the DATA to any third party, except as expressly permitted in this Agreement; or (ii) sell, lease, sublicense, copy or provide the DATA to any third party, except as expressly permitted in this Agreement.

4. **No Re-Identification**. The RECIPIENT shall not carry out any procedures with the DATA (linking, comparison, processing) with the intention to identify the DATA SUBJECT, unless requested by a DATA SUBJECT according to section III.6. below.

5. **Confidentiality.** Each PARTY shall treat the CONFIDENTIAL INFORMATION confidential for the duration of this Agreement, including any extension thereof, and thereafter for a period of five (5) years following termination or expiry of this Agreement. Excluded from this obligation of confidentiality shall be any CONFIDENTIAL INFORMATION of which one PARTY can reasonably demonstrate that it (a) was previously known to them, or (b) is, and/or becomes, publicly available during said five (5) year period through no fault of a PARTY, or (c) is independently and lawfully developed by one PARTY. This obligation of confidentiality shall not apply to any disclosure required by law, provided that the RECIPIENT shall notify the PROVIDER of any disclosure required by law in sufficient time so that the PROVIDER may contest such requirement, if the PROVIDER so chooses. Subject to mandatory law, upon the expiration or termination of this Agreement for whatever reason, or at the earlier request of a PARTY, the other PARTY shall, at its own costs, return or destroy all originals and copies of CONFIDENTIAL INFORMATION, or, in case of CONFIDENTIAL INFORMATION stored in electronic, magnetic or digital media, shall erase or render unreadable all materials furnished (including without limitation, working papers containing any CONFIDENTIAL INFORMATION or extracts therefrom) which contain CONFIDENTIAL INFORMATION.

6. **Rights of the DATA SUBJECT.** The PROVIDER shall secure the exercise of the DATA SUBJECT's rights, including access rights, the right to rectification and erasure, and the right to object. The PARTIES shall respond to requests from the DATA SUBJECT within one month after having received the notification. Moreover, the PARTIES will provide any DATA SUBJECT with a copy or the content of this Agreement upon their request or if required by law. In case of a production request by a DATA SUBJECT, either PARTY may summarize any part of this Agreement (including its Annexes) to the extent necessary for confidentiality and data protection reasons. Finally, any DATA SUBJECT may raise damages and other claims pursuant to the applicable law relating to the transfer and/or processing of their DATA under this Agreement against either PARTY.

7. **Revocation of Consent**. In case of DATA SUBJECT's total or partial revocation of consent, the PROVIDER must inform the RECIPIENT of this revocation without delay depending on the consent signed by the DATA SUBJECT and must provide the pseudo-identifier of the DATA SUBJECT that revoked access to his/her DATA. In such case, if applicable, the RECIPIENT shall comply with PROVIDER's requests to anonymize their DATA according to the HRO, unless one of the exceptions listed in Article 10 of the HRO applies. A written notification shall be sent to the PROVIDER upon receipt and after completion of the request.

8. **DATA Storage and Processing**. The DATA should not be kept by the RECIPIENT longer than necessary for the purpose of the RESEARCH, and the DATA processing must be limited to the purpose pursued, provided that the DATA SUBJECT does not decide otherwise.

9. **DATA transfer via the BioMed-IT infrastructure.** The PARTIES agree that the DATA transfer will be performed as agreed in writing by the technical representatives of the BIOMEDIT NODES, as set forth in **Annex III** of this Agreement and in accordance with all applicable laws.

## IV. Information about RESULTS and Publication

1. **Information about RESULTS**. Upon the PROVIDER's request, the RECIPIENT'S PROJECT LEADER shall keep the PROVIDER informed of the RESULTS. In case clinical actionable findings are identified according to good practice RECIPIENT'S PROJECT LEADER shall inform the PROVIDER.

2. **Publication**. The PARTIES shall jointly have the right, consistent with internationally accepted academic standards, to present and publish results of the RESEARCH, provided that any proposed presentation or publication (hereinafter, "Proposed Publication") has been submitted for review to the other PARTIES in accordance with this article.

   In the event of a Proposed Publication, the party in charge of the Proposed Publication shall provide the other PARTIES with a manuscript or draft presentation. The other PARTIES shall have fourteen (14) business days to review the same and to demand certain amendments as far as reasonably required to protect intellectual property rights and to maintain internationally accepted scientific standards. Both Parties shall consider the other's comments, if any, in good faith and amend the manuscript or draft presentation accordingly before making it public. In case the other Party does not respond within the fourteen (14) business-day period, the manuscript shall be deemed accepted by the Party.

   Any publication containing results partially or fully financed by SPHN must acknowledge SPHN as the funding source. The following acknowledgement form shows the minimal requirement: "This project was supported by the Swiss Personalized Health Network (SPHN) initiative."

   As SPHN projects are funded with public money, the Parties strive to make the resulting scientific publications publicly accessible and available through Open access as far as possible according to publishers rights.

   Further, the SPHN management office should be informed prior to any press releases related to SPHN project activities (info@sphn.ch).

3. **Authorship Guidelines**. All publications of the RESULTS must be compliant with the Authorship Guidelines of the Swiss Academies of Arts and Sciences, as updated from time to time, accessible at:

   http://www.akademien-schweiz.ch/en/dms/E/Publications/Guidelines-and-Recommendations/integrity/Academies_Authorship.pdf.

4. **Acknowledgements**. The RECIPIENT agrees to acknowledge the PROVIDER as the source of the DATA in all written publications, posters or oral presentations.

## V. INTELLECTUAL PROPERTY RIGHTS

1. **BACKGROUND IP**. The PARTIES agree that each PARTY shall retain all title, right and interest in and to its respective INTELLECTUAL PROPERTY RIGHTS, as of the date of entry into force of this Agreement (the "BACKGROUND IP"). Unless otherwise agreed herein, nothing in this Agreement shall be construed as a transfer, license, and/or assignment by a PARTY to the other PARTY of ownership of, title, right or interest in and to its respective BACKGROUND IP.

2. **FOREGROUND IP.** All right, INTELLECTUAL PROPERTY RIGHTS, title and interest in and to the RESULTS shall be owned jointly by the PARTIES (the "JOINT FOREGROUND IP"). The PARTIES will set forth, by separate mutual agreement, their respective rights, duties and responsibility relating to the JOINT FOREGROUND IP. Such an agreement shall not cause a delay of publication of the RESULTS any longer than as defined in Section IV.2.

## VI. Compliance

1. **Compliance with Law**. Each PARTY undertakes to comply at all time with all applicable Swiss laws, applicable international statutes, regulations and guidelines, especially all laws, statutes and regulations concerning human research and personal data protection, including any necessary regulatory approvals.

## VII. Expiration and Termination

1. **Expiration**. Subject to the approval of the appropriate ethics committee(s) if any, this Agreement shall become effective on the 01.11.2019, and it shall automatically expire at the completion of the RESEARCH 31.05.2024 (according to the research plan as described in **Annex II**) or at the termination of the RESEARCH for any reason.

2. **Termination**. Each PARTY may terminate this Agreement at any time by giving a three months prior written notice, unless a material breach of this Agreement by the other PARTY occurs. In such case, the PARTY that suffers the material breach may terminate this Agreement by written notice to the other PARTY, which is either incapable of remedy or has not been remedied within 30 days' notice from such breach. If the breach has not been rectified within said period, the other PARTY can terminate the breaching PARTY's participation with immediate effect and all rights granted to the breaching Party according to this Agreement, will cease immediately upon receipt of the formal termination notice. If the breaching PARTY is the PROVIDER, the PROVIDER shall continue to grant access to its DATA as if it had remained a PARTY for the whole duration of the PROJECT. However, it shall have no rights whatsoever to the RESULTS subsequently generated by the RECIPIENT after effective termination.

3. **Survival Clauses**. The provisions concerning CONFIDENTIAL INFORMATION, publications, INTELLECTUAL PROPERTY RIGHTS, warranty and liability as well as those intended to protect the rights of participants / DATA SUBJECTS shall survive the Agreement's expiration.

## VIII. Liability, Indemnification and Third-Party Rights

1. **Liability and Indemnification**. Each PARTY shall be liable to, and indemnify, the other PARTY for actual costs, charges, damages, expenses or losses suffered by the other PARTY resulting from any of the first PARTY's violation of this Agreement.

2. **Third Party Rights**. The PARTIES agree that a DATA SUBJECT shall have the right to enforce, as a third-party beneficiary, this Agreement against the RECIPIENT or the PROVIDER, for their respective breach of their contractual obligations, with regard to their DATA. In cases involving allegations of breach by the RECIPIENT, the PARTIES agree that the PROVIDER may take appropriate action to enforce their rights against the RECIPIENT. A DATA SUBJECT is entitled to proceed directly against the PROVIDER that has failed to use reasonable efforts to determine that the RECIPIENT is able to satisfy its legal obligations under this Agreement (the PROVIDER shall have the burden to prove that it took reasonable efforts).

3. **FOREGROUND IP**. The PARTIES use the FOREGROUND IP at their own risk. A PARTY using any of the FOREGROUND IP shall, to the fullest extent permitted by the applicable law, defend, indemnify and hold the other PARTY harmless against third party claims (including but not limited to claims based on mandatory product liability law) which are based on the PARTY's use of the FOREGROUND IP.

## IX. General Provisions

1. **Entire Agreement.** This Agreement represents this entire Agreement among the PARTIES with respect to the subject matter hereof, and may only be altered or amended by an instrument in writing signed by all of the PARTIES.

2. **Electronic Form**. The words "execution", "signature" and similar words in this DTUA shall be deemed to include unqualified electronic signature (e.g. Docusign or any equivalent e-signature provider) each of which shall be of the same legal effect, validity or enforceability as a manually executed signature, while the term "in writing" shall include communications by email.

3. **Severability and No Waiver**. If any portion of this Agreement is in violation of any applicable regulation, or is unenforceable or void for any reason whatsoever, it should be put in writing and discussed by the PARTIES. Such portion will be inoperative and the remainder of this Agreement will be binding upon the PARTIES.

4. **Governing Law and Jurisdiction**. This Agreement will be construed, governed, interpreted and enforced according to the laws of Switzerland. All disputes arising out of or in relation to this Agreement will be brought before the competent court at the seat of the defending PARTY. In case of disputes, the PARTIES will consult each other before taking any legal action.

5. **Contact Point:** The RECIPIENT'S PROJECT LEADER is the contact point within its organization, authorized to respond to enquiries concerning this Agreement, and will cooperate in good faith with the PROVIDER within a reasonable time.

## X. Annexes

**Annex I:** Data and Meta Data to be Transferred

**Annex II:** Research Project

**Annex III:** Data Transfer Specifications via the BioMedIT infrastructure

**Annex IV:** Minimal Security Requirement

**IN WITNESS WHEREOF**, the PARTIES have executed this Agreement as of the EFFECTIVE DATE.

**University Children's Hospital Zurich**

**Duly Authorized Representative**
Markus Malagoli
CEO
Date:

**Duly Authorized Representative**
Michael Grotzer
Prof. Dr. med.
Clinical Director
Date:

**RESEARCH Project Leader**
Christoph Berger
Prof. Dr. med.
Date:

**University Children's Hospital Basel**

**Duly Authorized Representative**
Sven Schulzke
Prof. Dr. med.
Date:

**Duly Authorized Representative**
Urs Frey
Prof. Dr. med.
Clinical Director
Date:

**Project Leader**
Julia Bielicki
Dr. med.
Date:

**University of Basel**

**Duly Authorized Representative**
Torsten Schwede
Prof. Dr.
Head of Research
Date:

**Project Leader**
Henriette Meyer zu Schwabedissen
Prof. Dr. med.
Date:

**ETH Zurich**

**Duly Authorized Representative**
Detlef Günther
Prof. Dr.
Vice President for Research
Date:

**Project Leader**
Stefanie Krämer
Prof. Dr.
Date:

# ANNEX I: DATA AND META DATA TO BE TRANSFERRED

The following DATA and metadata shall be provided from PROVIDER to RECIPIENT:

All health-related personal data and biological material of patients, who have agreed to their further use in the general consent and who are treated with the relevant drugs for the *Swiss Pharmacokinetics clinical data warehouse (SwissPK$^{cdw}$)* SPHN Project here referred by as RESEARCH.

DATA and metadata are stored in the PROVIDERs various source systems. DATA and metadata are extracted from the source systems, pseudonymized, encrypted and transferred securely to the RESEARCH clinical data warehouse on Leonhard Med. Leonhard Med is a new secure scientific IT platform provided by ETH Zurich to store, manage, compute on and share confidential biomedical research data. All users authorized to access Leonhard Med must abide by the Leonhard Med Acceptable Use Policy (https://rechtssammlung.sp.ethz.ch/Dokumente/438.1.pdf), a binding document whose purpose is to prevent breach of confidentiality, integrity, or availability of sensitive Personal Data, or other confidential research data, entrusted to the Leonhard Med system. Leonhard Med is one of the nodes in the emerging BioMedIT network of secure Data and IT infrastructures, supporting the SPHN projects in Switzerland.

Once transferred within the secure RESEARCH project space on Leonhard Med, the pseudonymized DATA is decrypted. During the project duration, the DATA is backed up on a daily basis (encrypted and geo-redundant backup).

# ANNEX II: RESEARCH PROJECT

The RESEARCH shall be limited to use of the DATA in connection with the following activities:

For the SPHN infrastructure project *Swiss Pharmakokinetik clinical data warehouse* (*SwissPK$^{cdw}$*) here referred to as RESEARCH (PI Prof. Dr. med. Christoph Berger) a clinical data warehouse is going to be created on the Leonhard Med ETH Zurich.
The project goal is the individual dosage of drugs in children based on clinical parameters (DATA from the PROVIDERS). By creating this clinical database (RESEARCH) enough parameters are made available to create practical dosage equations for children using a pharmacokinetic model.

The DATA from the PROVIDERS (University Children's hospital Zurich [KISPI], University Children's Hospital Basel [UKBB], University of Basel) will be stored in pseudonymized form on the RESEARCH clinical data warehouse (CDW). The CDW will be hosted in the secure dedicated space for this project on Leonhard Med IT and used for pharmacokinetic modelling.

For the RESEARCH the patient's health DATA will be extracted from the source systems of the pediatric hospitals (UKBB, KISPI). From UKBB and KISPI, predefined clinical and patient-related DATA of the relevant drugs are validated, pseudonymized (encoded) encrypted and transferred via the secure IT node sciCORE [DATA from Basel] and ETH:SIS [DATA from Zurich] to the Leonhard Med ETH, following the secure data transfer protocol of the BioMedIT network. KISPI sends pseudonymized biological samples from patients receiving a RESEARCH relevant drug to the University of Basel, were the samples are analyzed for predefined polymorphisms. The resulting (Genetic) DATA of the polymorphism analysis at the University of Basel is then encrypted and transferred via the sciCORE node to the Leonhard Med IT node. The decryption and the upload of the DATA into data management software openBIS on Leonhard Med is at the beginning manually (then automatically) performed by the data manager of the RESEARCH. Once in openBIS, the pseudonymized DATA can be exported into R for future pharmacokinetic (PK) modelling by RECIPIENT'S (University of Basel, ETH and KISPI). A login is required to access the RESEARCH, which will be provided by the BioMedIT Node ETH:SIS and approved by the RESEARCH PI. The users of the RESEARCH will additionally need to pass the SPHN Data Privacy and IT Security Training, sign the *SwissPK$^{cdw}$* and AUP of Leonhard Med secure HPCI (LM) policies and obtain an ethical approval for doing research with specific DATA. The specialized data management open source software openBIS provides extensive audit trails for DATA, i.e., all modifications made to any entity (i.e., DATA) in the openBIS system are recorded, stored in a database and can be used for data provenance tracking.

Confidential pseudonymized DATA on the openBIS can only be exported from the project space to external endpoints under strict authorization of the RESEARCH, following the security specification of the Leonhard Med Acceptable Use Policy.

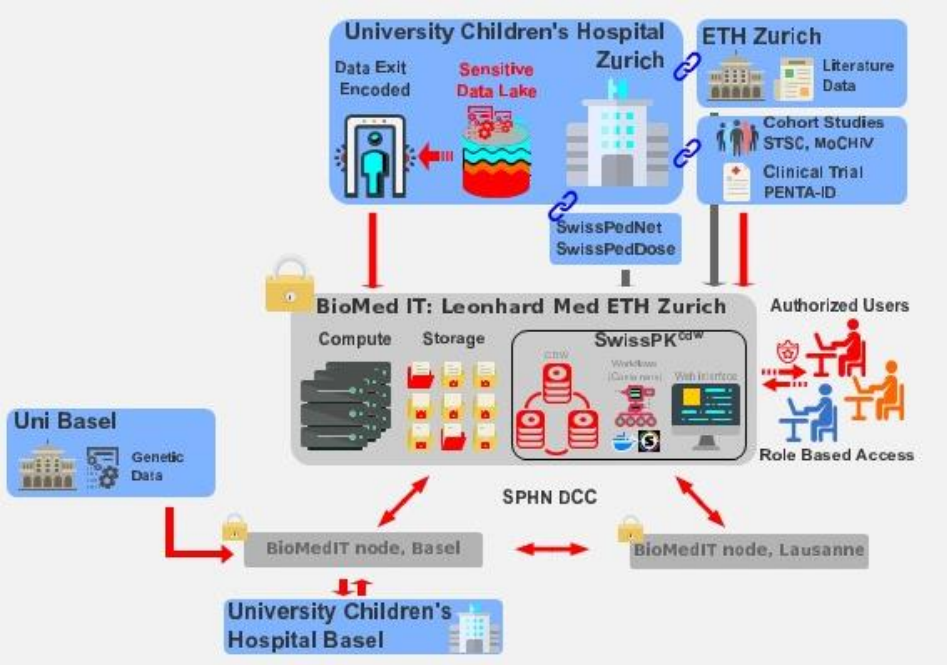


***Figure 1:*** **Schematic representation of the secure data-handling plan.**
The various data sources are shown in blue boxes. The arrows indicate the direction of the data transfer and the colors distinguish between non-sensitive data (grey) and sensitive data (red: indicates the main direction for data transfer). Source: Research Plan SPHN, figure created by: Diana Coman, figure modified by: Vera Jäggi

# ANNEX III: BIOMEDIT INFRASTRUCTURE DATA TRANSFER AND PROCESSING AGREEMENT

(the "**DTPA**")

between

**University Children's Hospital Basel**, Spitalstrasse 22, CH - 4056 Basel

and

**University Children's Hospital Zurich**, Steinwiesstrasse 75, CH - 8032 Zurich

and

**University of Basel**, Hebelstrasse 20, CH - 4031 Basel

and

**ETH Zurich**, Hauptgebäude, Rämistrasse 101, CH - 8092 Zurich

---

(the "**PROVIDER**" and "**RECIPIENT**", together the "**PRINCIPALS**")

and

**University of Basel** (SciCore, Basel BioMedIT Node) Petersplatz 1, Postfach, CH - 4001 Basel

**ETH Zurich** (Scientific IT Services - SIS, Zurich Node), Hauptgebäude, Rämistrasse 101, CH - 8092 Zurich

---

(together the **BIOMEDIT NODES**)

(for the purposes of this Agreement, each a **PARTY**, and the **PARTIES**)

---

**WHEREAS**

a) The PRINCIPALS have signed a Data Transfer and Use Agreement for the SPHN Infrastructure Project "*SwissPK$^{cdw}$: Optimizing pediatric dosage regimens based on a clinical data warehouse"* (the **DTUA**).

b) The BIOMEDIT NODES form together a coordinated Swiss nationwide network of secured IT network (the **BIOMEDIT NETWORK**), consisting of high performance compute and storage infrastructure, in order to support computational biomedical research and clinical bioinformatics.

c) Within the framework of its access and use of DATA, the PRINCIPALS wish to benefit from the BIOMEDIT NODES services to *inter alia* store and transfer DATA from PROVIDER to RECIPIENT.

d) The BIOMEDIT NODES agree to provide such services under the terms and conditions of this DTPA.

---

## I. DEFINITIONS

Except as otherwise defined in this DTPA, capitalized terms, whether used in singular or plural form, shall have the same meaning as set forth in the DTUA.

## II. SCOPE

This DTPA applies to all DATA, including personal DATA relating to any concerned DATA SUBJECTS, that are transferred to and processed by the BIOMEDIT NODES in the name and on behalf of the PRINCIPALS under the RESEARCH and the DTUA.

## III. SERVICES

1. **In General**. Subject to, and in accordance with, the terms of this DTPA, each REGIONAL NODE undertakes to provide to the PRINCIPALS the services specified in Section 2.2 (the **SERVICES**) to the best of its ability using all reasonable skill and care, and always subject to the PRINCIPALS' compliance with all its obligations under this DTPA.
2. **Scope**. The SERVICES consist of, except as otherwise specified in Appendix 1, the following:
   a) hosting of the DATA on the BIOMEDIT NETWORK;
   b) transferring DATA from the PROVIDER to the RECIPIENT in accordance with this DTPA; and
   c) other processing activities as required under this DTPA or as reasonably requested by the PRINCIPALS.
3. **Means of Transfer**. Except as otherwise agreed in writing, DATA shall be transferred by providing to the RECIPIENT remote secured access to the DATA in accordance with the security standards specified in Section IV.3.1 below. The PARTIES shall decide on a case by case basis from which REGIONAL NODE the DATA shall be made available.
4. **Collaboration with and between REGIONAL NODES**. SERVICES are provided by the REGIONAL NODES as described in **Appendix 1**. The Parties shall specify in **Appendix 1** which REGIONAL NODE shall be primarily responsible for providing the SERVICES. Each REGIONAL

NODE undertakes to collaborate with the other REGIONAL NODES, and to assist them, as may be required for the proper providing of the SERVICES.

5. **Power**. The PROVIDER'S PROJECT LEADER and the RECIPIENT'S PROJECT LEADER shall have the individual power to give instructions to, and receive notification from, the BIOMEDIT NODES, on behalf of, respectively, the PROVIDER and the RECIPIENT, for all actions relating to the DATA.

## IV. DATA PROCESSING TERMS

1. **Supply of Data.** PROVIDER shall provide the DATA to the selected REGIONAL NODE, or make the DATA available to it, in the form and as specified in **Appendix 1**.

**2. Scope of Processing**

**2.1.** In General. The Parties acknowledge and agree that:

a) the subject matter and details of the processing are specified in this DTPA and its **Appendix 1**;

b) the BIOMEDIT NODES are joint processors of the DATA;

c) the PRINCIPALS are joint controllers of the DATA; and

d) each PARTY shall comply with its obligations under any applicable laws with regard to the processing of the DATA (including data protection laws, as well as laws, statutes and regulations concerning human research and personal data protection).

**2.2.** Nature and Purpose of Processing. The BIOMEDIT NODES shall process the DATA on behalf of the PRINCIPALS and solely for the purpose of providing the SERVICES or as otherwise expressly instructed jointly by the PROVIDER'S PROJECT LEADER and the RECIPIENT'S PROJECT LEADER. For the sake of clarity, the BIOMEDIT NODES shall have no obligation to carry out any instruction which they consider, at their sole discretion, to be unlawful, ambiguous, doubtful or unclear (in which case the PARTIES shall collaborate in good faith to find a solution agreeable to all).

**2.3.** Restrictions. The BIOMEDIT NODES shall not, without the prior written consent of PROVIDER:

a) subcontract any of their processing operations of the DATA (except to another REGIONAL NODE); and

b) transfer the DATA in any country outside Switzerland (it being agreed that the DATA may be accessed and processed by the PRINCIPALS outside Switzerland, in which case they shall be responsible for compliance with any applicable data protection obligation).

**2.4.** Return of DATA. Upon termination of the DTPA, or earlier as requested by the PROVIDER, the BIOMEDIT NODES shall, within reasonable time following a written request by PROVIDER, provide PROVIDER with a final extract of the DATA and permanently delete all copies of such DATA still under its control. In any case, the BIOMEDIT NODES shall be allowed to permanently delete the DATA 60 days after termination of the DTPA.

**3. Security**

**3.1.** Security Requirements. Each PARTY shall comply with the security requirements set forth in Section III.C.3 of the DTUA.

**3.2.** Security Incidents. Each REGIONAL NODE processing DATA shall, if it becomes aware of any accidental or unauthorized access to the DATA, inform the PRINCIPALS as soon as possible by any useful means (in particular via the PROVIDER'S PROJECT LEADER). The REGIONAL NODE shall, to the extent possible, describe the nature of the security incident, as well as any measures taken by it to mitigate potential risks and the measures that it recommends the PRINCIPALS to take. The PRINCIPALS shall be responsible for complying with the legal provisions applicable to them, in particular any obligations of the PRINCIPALS to provide a notification of the incident to any competent authority and/or the DATA SUBJECTS. In this context, the REGIONAL NODE shall provide the PRINCIPALS with any assistance reasonably required by them in order to comply with their obligations.

**4. Register of Processing Activities**

**4.1.** The PRINCIPALS acknowledge that the BIOMEDIT NODES may be required to:

a) collect and store certain information, including the name and contact details of each processor and/or controller with whom the BIOMEDIT NODES act and, where applicable, the local representative of the controller and/or the data protection officer as well as the categories of processing carried out; and

b) make such information available to any competent authority.

**4.2.** The PRINCIPALS undertake to provide the BIOMEDIT NODES with all information reasonably necessary for the BIOMEDIT NODES to meet their obligations.

## V. REPRESENTATIONS AND WARRANTIES

5. The PRINCIPALS represent and warrant that:

a) the DATA to be transferred to and processed by the BIOMEDIT NODES has been collected, transferred and processed in accordance with the requirements of all applicable laws, rules and regulations, including all applicable data protection laws and regulations;

b) the transfer to the BIOMEDIT NODES and the processing of the DATA by the BIOMEDIT NODES (including any further transfer to the RECIPIENT) as set forth in this DTPA is (i) admissible under all applicable laws, rules and regulations and (ii) is not prohibited by a statutory or contractual duty of confidentiality;

c) prior to any collection, transfer, or processing of personal data, the PRINCIPALS have provided to the concerned DATA SUBJECTS all required information (including in relation to any processing activity contemplated under this DTPA) and complied with any notification and registration obligations under any applicable laws and regulations;

d) the PRINCIPALS will not require the BIOMEDIT NODES to undertake a processing of DATA that they would not be permitted to carry out themselves.

e) they have and will verify that the technical and organizational measures, as required by all applicable laws, rules and regulations, undertaken by the BIOMEDIT NODES, in particular with those specified in Section III.C.3 of the DTUA, are sufficient to protect the transferred and processed DATA from any unauthorized processing. The PRINCIPALS warrant that the technical and organizational measures set forth in Section III.C.3 of the DTUA are sufficient in this regard.

## VI. INFORMATION, ASSISTANCE AND NOTIFICATIONS

1. **Compliance**. Each PARTY shall provide the other PARTIES with all the necessary information so that they can demonstrate compliance with their obligations under applicable Swiss or European data protection legislation.
2. **Rights of the Concerned DATA SUBJECTS**. The PRINCIPALS are responsible that the concerned DATA SUBJECTS are provided with their right of access, rectification, deletion or objection. The BIOMEDIT NODES will fully and in a timely fashion cooperate with the PRINCIPALS in, and when applicable provide to the PRINCIPALS the necessary services for, fulfilling such requests or inquiries of the concerned DATA SUBJECTS.
3. **Impact Assessments and Prior Consultation**. The BIOMEDIT NODES undertake, to the extent they can reasonably be expected to do so in light of the nature of the processing and the information available to them, to assist the PRINCIPALS in ensuring its compliance with its impact assessment and prior consultation obligations.
4. **Notification and Assistance**. The BIOMEDIT NODES shall promptly inform, and cooperate with, the PRINCIPALS if they believe that they may no longer be able, or are no longer able, to comply with this DTPA, particularly in case they receive or must reasonably expect to receive a request or order of a competent authority requiring them to disclose, or refrain from further processing, some or all personal DATA to which this DTPA applies.

## VII. DATA OWNERSHIP, INTELLECTUAL PROPERTY, CONFIDENTIALITY

### 1. Data Ownership and Right to Use

a) Ownership. As between the PRINCIPALS and the BIOMEDIT NODES, and without prejudice to the DATA SUBJECTS' rights to the DATA pursuant to applicable laws on data protection and on Human research, all rights to the DATA are and remain the property of the PRINCIPALS and all right, title, and interest in the same (including any INTELLECTUAL PROPERTY RIGHT) is reserved by the PRINCIPALS. Subject to Section VII.1.b) below, nothing in this DTPA is intended to assign or grant the BIOMEDIT NODES any INTELLECTUAL PROPERTY RIGHTS or other rights in the DATA.

b) Use of DATA. The PRINCIPALS grant to the BIOMEDIT NODES a right to access and use the DATA for the sole purpose of, and only to the extent necessary for, providing the SERVICES, including a license to collect, process, store, generate, and display the DATA.

c) Acceptable Use Policy. The PRINCIPALS undertake to comply with the *Acceptable Use Policy* specific to each REGIONAL NODE.

2. **Confidentiality.** Each PARTY shall comply with the provisions of Section III.5 of the DTUA in relation the all CONFIDENTIAL INFORMATION, which term shall include for the purpose of this DTPA all data, document, or other material (in any form) of the BIOMEDIT NODES that is identified as confidential at the time it is disclosed by a REGIONAL NODE to another PARTY hereunder.
3. **IP in BIOMEDIT NETWORK**. As between the PRINCIPALS and the BIOMEDIT NODES, the BIOMEDIT NODES shall be and remain the sole owner of all INTELLECTUAL PROPERTY RIGHTS in and to the BIOMEDIT NETWORK, as well as any other infrastructure used to provide the SERVICES. Nothing in this DTPA is intended to assign or grant THE PRINCIPALS or any other party any INTELLECTUAL PROPERTY RIGHTS or other rights in the BIOMEDIT NETWORK.

## VIII. LIABILITY AND INDEMNIFICATION

1. Subject to Section VIII.2 below, each PARTY shall be liable to, and indemnify, the other PARTIES for actual costs, charges, damages, expenses or losses suffered by the other PARTIES resulting from its breach of any of its obligation or warranty under this DTPA.
2. Each PARTY disclaims any liability for any indirect damages or losses, whether foreseen or foreseeable, related to the loss of use, interruption of business, loss of actual or anticipated profit, loss of revenue, loss of anticipated savings, loss of opportunity, loss of goodwill, loss of reputation, loss of, damage to or corruption of assets or data, or any other indirect, incidental, exemplary, or consequential damages or losses of any kind, regardless of the form of action, whether in contract, tort or otherwise.

## IX. TERM

1. **Term**. This DTPA shall be binding between the PARTIES upon its execution by all PARTIES and shall remain in effect until expiration or termination of the DTUA, unless terminated earlier in accordance with this Section of IX of the DTPA.
2. **Termination for Convenience**. Each PARTY may terminate this DTPA for any reason at any time upon 3 months prior written notice to the other PARTIES. A termination by a PARTY shall have the effect of terminating the DTPA for all PARTIES, except as otherwise agreed in writing by the non-terminating PARTIES.
3. **Termination for Cause**. Each PARTY may terminate the DTPA with immediate effect, if another PARTY has materially breached or is in material breach of its obligations and such breach is not cured, or the breaching PARTY is not diligently pursuing a cure, within 30 days after written notice of breach.
4. **Survival**. All terms which are expressed or intended to survive, and any provisions of the DTPA necessary for its interpretation or enforcement will continue to apply regardless of the reason for termination of the DTPA.

## X. MISCELLANEOUS

1. **Amendment**. This DTPA may be modified only by a written instrument duly executed by each PARTY.
2. **Independent Contractors**. Nothing in this DTPA is intended to, or shall be deemed to, establish any partnership or joint venture between the PARTIES, constitute any PARTY the agent of any other PARTY, nor authorize any PARTY to make or enter into any commitments for or on behalf of another PARTY. No PARTY shall have the power to incur any obligations in the name of, or on behalf of, or pledge credit of, the other PARTIES in any manner whatsoever.
3. **Electronic Form**. The words “execution”, “signature” and similar words in this DTPA shall be deemed to include unqualified electronic signature (e.g. Docusign or any equivalent e-signature provider) each of which shall be of the same legal effect, validity or enforceability as a manually executed signature, while the term "in writing" shall include communications by email.
4. **Assignment**. No PARTY may transfer this DTPA, or assign in whole or in part its rights or obligations under this DTPA, without the prior written consent of all other PARTIES. Any transfer or assignment made without such consent shall be null.
5. **Force Majeure**. No PARTY shall be considered in default under this DTPA if all or any of its obligations are delayed or prevented as a result of a situation of force majeure, such as natural

disasters of a particular intensity, war, epidemics, riot, strike, power failure or Internet network failure, or any other cause that is reasonably beyond the control of the affected PARTY.

6. **Entire Agreement**. This DTPA contains all of the terms and conditions agreed upon by the PARTIES relating to its subject matter and supersedes all prior agreements, negotiations, correspondence, undertakings and communications of the PARTIES, whether oral or written, with respect to such subject matter.

7. **Hierarchy**. In the event of conflict with a schedule to this DTPA, this main body of this DTPA will govern, unless the schedule specifically states its intent to do so and cites the section or sections amended.

8. **Severability**. If any provision of this DTPA is held to be invalid or unenforceable for any reason, the PARTIES shall replace it by a substitute provision that achieves to the fullest extent possible the same legal and economic purposes as those of the invalid or unenforceable provision. In any event, the remainder of this DTPA shall remain in full force and effect between the PARTIES.

9. **No Waiver**. The failure of any of the PARTIES to enforce any of the provisions of this DTPA or any rights with respect thereto shall in no way be considered as a waiver of such provisions or rights or in any way affect the validity of this DTPA. The waiver of any breach of this DTPA by any PARTY shall not be construed as a waiver of any other prior or subsequent breach.

## XI. GOVERNING LAW AND JURISDICTION

1. **Governing Law.** This DTPA shall be governed by and construed in accordance with Swiss substantive law, without reference to its conflict of laws provisions.

2. **Jurisdiction**. Any dispute or difference arising out of or in relation to this DTPA shall be subject to the exclusive jurisdiction of the Swiss courts at the registered seat of the defending PARTY, subject to the right of appeal to the Federal Tribunal.

**Acknowledged and approved by the BioMedIT Nodes**

**University of Basel** (sciCORE, Basel BioMed-IT Node)

_____

Torsten Schwede
Vice-Rector of Research
Date:

_____

Thierry Sengstag
Deputy director - sciCORE computing center
Date:

**ETH Zurich** (Scientific IT Services - SIS, Zurich Node)

_____

Bernd Rinn
Head of SIS
Date:

_____

Rui Brandao
Director IT Services
Date:

**Appendix 1 to the DTPA – Description of DATA and SERVICE**

## A. Description

See Annex I to the DTUA.

SIS ETHZ (Leonhard Med) is the main BioMedIT Node for this project (concerning the hosting and processing of data). sciCORE and Core-IT will only transfer data from PROVIDERS to SIS ETHZ.

## B. Supply of DATA to the BIOMEDIT NODES

Transfer of Data

Data will be transferred to the BioMedIT Nodes within a standardized and secure way, i.e. using the network-internal Data Transfer Tool. Data is stored and processed in compliance with the SPHN Information Security Policy.

Data access

The RESEARCH PROJECT LEADER defines who will be authorized to access the DATA. Access of authorized users to the project space requires two-factor authentication. Furthermore, authorized users can only access the infrastructure from within trusted IT environments (either from within a Swiss university network, a university hospital network or via VPN).

# ANNEX IV: MINIMAL SECURITY REQUIREMENT

RECIPIENT shall ensure that the technical and organisational measures provided by the Data Processor are sufficient to guarantee the confidentiality, integrity, availability and resilience of the systems with regard to processing of data. In particular, the RECIPIENT must:

- deny unauthorized persons access to facilities and data processing systems;
- ensure that unauthorised persons are prevented from reading, copying, altering or deleting data in/from data processing systems;
- ensure that unauthorized persons are not able to read, copy, modify or remove data upon the electronic transfer of data as well as during the transport of data carriers or saving of data thereon;
- ensure that it is possible to examine and verify if, when and by whom data was entered into the data processing system;
- ensure that data is protected from accidental destruction or loss;
- ensure that data received is not combined with other data unless explicitly authorized by the competent ethics commission for the specific research project;
- restrict the disclosure and handling of data to those persons who require it to conduct the specified research project and to be able to identify each of them;
- ensure adequate organisational measures to protect data, especially by selecting, instructing and supervising employees involved in the processing of data diligently and appropriately, by guranteeing the availability of: adequate confidentiality and data protection guidelines, regular data protection and privacy trainings, documentatio of all organisational measures;
- ensure that the effectiveness of technical and organisational measures is regularly reviewed and assessed.
- implement corrective measures and immediate reporting in case of any suspected data security breach.