SwissPK^{cdw} User Policy

Content

1. General Provisions

1.1 Purpose of Policy

The purpose of this policy is to provide to all *SwissPK^cdw* team members an easy-to-read overview of their responsibilities and obligations regarding the processing and handling of confidential research data generated by the *SwissPK^cdw* project. This policy applies to all users authorized to access and use the *SwissPK^cdw* project space and resources hosted at Leonhard Med (e.g., *SwissPK^cdw* data storage, openBIS, web app). The content of the *SwissPK^cdw* policy is based on The Acceptable Use Policy (AUP) of the Leonhard Med secure High Performance Computing Infrastructure policy. Therefore, reading this document includes reading the Leonhard Med AUP policy referenced in the Appendix. By signing the policies (4.4 in the appendix), the users agree on the policies contents. Reading this document does not replace reading other applicable laws and regulations.

1.2 Definitions

"SwissPK^cdw" **S**wiss **P**harma**K**okinetics **c**linical **d**ata **w**arehouse is a **S**wiss **P**ersonalized **H**ealth **N**etwork (SPHN) infrastructure project. The projects aim is to optimize pediatric dosing regimens based on pharmacokinetic modelling with personal health data registered in a newly generated clinical data warehouse (cdw). This cdw is hosted at Leonhard Med (LM), a node of the BioMedIT secure scientific IT infrastructure for confidential research data, supporting SPHN projects.

The term "*data"* includes personal data, confidential data, internal data and public data.

"*Personal data"* is defined as "*all information relating to an identified or identifiable person*" by the Swiss Federal Act on Data Protection (FDPA[1]). Personal data includes, but is not limited to: name, gender, birthdate of a natural person.

"*Confidential data"* is used as defined in the AUP LM[2] and it refers to sensitive personal data as defined in FADP. Accordingly, confidential data include, data about a person's religion, health, social security measurements, administrative or criminal proceedings and sanctions. In particular, all health-related or medical data (either identifying or pseudonymized data) classify as confidential, unless explicitly classified differently. "*The impact of such data leaking to parties without rightful and legitimate use or to the public may cause major harm to the person from whom the data originate, to the original Data Provider (Controller), to the research organization, or to ETH Zurich.*[2]"

"*Internal Data*" is used as defined in the AUP LM[2]. Accordingly, internal data refers to "*information intended for members of ETH Zurich, or for all project partners of a project using Leonhard Med*", thus including information related to the *SwissPK^cdw* users (e.g. project related financial information, user e-mails, research data explicitly classified as internal).

A "*User"* is a person that is authorized to use the *SwissPK^cdw* tenant on Leonhard Med. To be allowed to use the *SwissPK^cdw tenant*, the user must:

I. Pass the SPHN Data Privacy and IT security test
II. Read, understand and sign the *SwissPK^cdw* and the AUP of LM policy (Appendix 4.4).
III. Get explicit authorization by the *SwissPK^cdw* project leader

[1] https://www.admin.ch/opc/en/classified-compilation/19920153/index.html

[2] AUP of LM https://rechtssammlung.sp.ethz.ch/Dokumente/438.1.pdf

An *"Endpoint,"* as stated by the AUP LM[3] Art 2 (5) is a "*computerized device connected to Leonhard Med by a network*". The notebook, laptop, tablet of a user is by those means an Endpoint of Leonhard Med. The IT security Guideline policy from ETHZ LM[4] forbids automatic login features, obligates to use malware software, recommends hard disk and home directory encryption, disabling whenever possible Bluetooth and WLAN and suggest checking regularly for security patch updates on the endpoint. For further information, please read the policy on IT Security Guidelines for ETH Zurich Leonhard Med Endpoints[4].

A "*tenant"* in Leonhard Med consists of separate network space containing access, computing and data resources, protected by its own set of firewall rules. The responsibility of use and access lies with the Project Leader (PL)[3].
The *SwissPK^cdw* project uses such a secure isolated tenant in Leonhard Med.

"*openBIS*"[5] is a data management system developed and provided by the Scientific IT Services of the ETH Zurich, which allows data provenance track, changelog and user rights management. A dedicate openBIS instance for this project is installed in the *SwissPK^cdw* tenant in Leonhard Med. Specifically, a custom data model designed for this project is used, including possibility of separate spaces for each drug. Access to openBIS within the *SwissPK^cdw* tenant in Leonhard Med can be further restricted to selected authorized users, including restricted access to specific drug spaces within openBIS (user rights management), based on their legal authorization (ethical approval).

The term "*project leader (PL)"* is defined as the person responsible and accountable for the *SwissPK^cdw* project (i.e., the main funding applicant). The project leader can delegate tasks but the final responsibility for the project lies with the project leader. According to the AUP LM[3] the PL "*denotes the person responsible for organizing a research project on Leonhard Med and leading it scientifically*".

The *"project data manager"* (*PDM),* is an assigned role by the PL with the responsibilities of secure data transfer and data management during the project duration. PDM is responsible for example to format, harmonize, validate, encrypt, transfer, decrypt and register data. Incorrect data records or data plots on the *SwissPK^cdw* tenant are validated and the SwissPKcdw PDM initiates respective correcting processes.

A "*computational workflow developer"* is an authorized project member, which interacts with the openBIS instance in the *SwissPK^cdw* tenant and with other relevant software and applications centrally provided at Leonhard Med. The computational workflow developer has access to a drug space in the project openBIS instance, according to the ethical approval for the specific drug. An example: the data exported from openBIS and imported into R are the base of the pharmacokinetic modelling and the resulting dosage recommendations, which can be displayed later on in the web app.

The *"web app"* is a tool where authorized project members can either explore the drug reports or obtain dosage recommendation for a selected drug, Exploring reports or dosage recommendations in the web app do not contain any confidential data. Information displayed on the web app are derived based on the confidential data managed and analyzed with openBIS and R, respectively. The data displayed are statistical summaries, a proposed loading/maintenance dose or a plasma concentration. These are aggregated data and do not display patient level information. As the *SwissPK^cdw* web app uses as input for analyses confidential research data, it is hosted within the *SwissPK^cdw* tenant in Leonhard Med and accessed by users via remote desktop of Leonhard Med using a two-factor authentication.

[3] AUP of LM https://rechtssammlung.sp.ethz.ch/Dokumente/438.1.pdf
[4] IT Security Guidelines for ETH Zurich Leonhard Med Endpoints https://rechtssammlung.sp.ethz.ch/Dokumente/438.2.pdf
[5] https://sis.id.ethz.ch/software/openbis.html

A *"web app user"* is an authorized project member interacting with the web app.

An "entity" represents a real world object or aspect in the data model. In the *SwissPK^cdw* Project the entities are "patient", "diagnosis", "lab result", "medication", "measurement", "genetics". Each entity consists of attributes, e.g. [measurement_value] is an attribute of the entity "measurement". According to the entities, the spaces in the openBIS data model are filled with confidential data.
E.g. the entity **measurement** consists of the following attributes:

[data_provider_institute]	[subject_pseudo_id]	[measurement_value]	[measurement_unit]	[measurement_datetime]

A "*data record"* is a collection of the specific attribute values of a specific instance of an entity, for example for a single measurement:

[data_provider_institute]	[subject_pseudo_id]	[height_measurement_value]	[height_measurement_unit]	[height_measurement_datetime]
CHE-101.525.004	BFGH13FZHI22	135	cm	2019-04-02T10:40:13

"encryption" is the *"usage of cryptographic methods to make data only accessible to legitimated Users in possession of a cryptographic key and/or a secret"*.[6]

"*Coded"* is defined in the SPHN glossary[7] as the linkage of personal health and biomaterial data via code to a specific person. In the *SwissPK^cdw* "*pseudonymization*" is used instead of "*coded"* and is defined as the following: *"pseudonymization[8]"* of data is the process of removing the identifying attributes of a data record or replacing them with a de-identified value. For the *SwissPK^cdw* data this means that name and first name of patients are erased, the Hospital-Patient-ID is replaced by a subject pseudo ID and all the timestamps = *datetimes* (incl. birth date) are provided with a patient specific offset. The mapping table for pseudo patient IDs and date offsets are only accessible to a designated person in the data providing hospital.

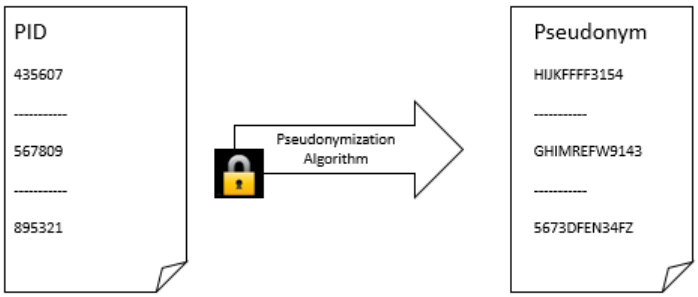

Fig.1: Pseudonymization. The patient identification number/identity (PID) is randomly replace with a different code based on a pseudonymization algorithm. The pseudonymization algorithm is password protected.

[6] AUP of LM https://rechtssammlung.sp.ethz.ch/Dokumente/438.1.pdf
[7] https://sphn.ch/wp-content/uploads/2019/11/Glossary_20180530_SPHN-1.pdf
[8] https://gdpr-info.eu/art-4-gdpr/

2. Use

2.1 Purpose and Scope of Use

The *SwissPK^cdw* project has the scope to build a research platform to optimize pediatric dosing regimen based on pharmacokinetic modelling conducted by developers.

2.2 No Private Use

Based on the AUP of the Leonhard Med secure HPCI (LM), the Leonhard Med cluster must not be used for any private projects, which has not been approved by the Ethical committee and ETH Zurich as the provider of Leonhard Med.

2.3 Data Classification

All data in stored in the *SwissPK^cdw* tenant in Leonhard Med and managed therein with openBIS classify as confidential. The data displayed on the *SwissPK^cdw* web app user interface contain non-confidential data. E.g., statistical summaries of data records are shown and no patient-level information are displayed.

2.4 Processing of Confidential Data

To access the *SwissPK^cdw* tenant in Leonhard Med and the custom project services therein (e.g. openBIS, web app), users must:

I. Pass the SPHN Data Privacy and IT security test
II. Read, understand and sign the *SwissPK^cdw* and the AUP of LM policy (Appendix 4.4).
III. Get explicit authorization by the *SwissPK^cdw* project leader

Furthermore, to access a specific drug data registered in openBIS within the *SwissPK^cdw* tenant "*computational work-flow developer" Users* require explicit authorization in agreement with the ethical approval for the respective drug.

2.5 Rights and Obligations

2.5.1 Leonhard Med

According to the AUP LM[9] Art. 9-10, the PL is responsible for the correct classification of Data, the authorization of transmission of confidential data to endpoints and of ensuring that all legal bases are fulfilled when it comes to the data cycle (including data storage and handling). Further, the PL is responsible to maintain a list of authorized project users (e.g., name, mail, position in project) who have requested access, signed the policies and are currently working on the tenant. The PL ensures that all documents, including legal aspects of the project as well as the regulations of data processing, are available.

2.5.2 SwissPK^cdw

It is strictly forbidden to copy confidential research data (including but not limited to secure copy protocol (scp[10]), copy/paste or use of the print screen functionality) from the *SwissPK^cdw* tenant onto the User's computers (endpoints), irrespective if the data is accessed via the file system, openBIS or displayed in the web app.

Failure to comply with this rule will result in immediate revocation of authorization to access the *SwissPK^cdw* tenant as well as legal consequences.

Any breach of confidential data must be immediately reported by the PL to the Leonhard Med service team (mailto: servicedesk@id.ethz.ch) as well as to the *SwissPK^cdw* (mailto: SwissPKcdw@kispi.uzh.ch).

9 AUP of LM https://rechtssammlung.sp.ethz.ch/Dokumente/438.1.pdf

10 https://www.pcwdld.com/what-is-scp

3. Feedback on Uncertain Data Records or Plots on *SwissPK^cdw*

3.1 Web App

The display of drug reports may contain errors such as wrong axis naming, failure in displaying plots, incorrect statistics etc. If such an incorrectness is visible, the web app user will be able to give feedback with tools provided on the web app.

3.2 openBIS

If incorrect data records are identified in openBIS (for example unrealistic values, 500 kg as a weight value measurement), the developer can give tenant internally a feedback on the incorrect data record.

4. Appendix

4.1 Project Role Assignment

Project Role	Assignment
Project leader	Prof. Dr. med. Christoph Berger
Co-Project leader	Dr. med. Paolo Paioni
Project data manager	Vera Jäggi

4.2 Document Changes

Document Version:	Version 1.0
Effective Date:	09.06.2020
Applicability:	01.06.2020
Document editor:	Diana Coman Schmidt | 28.04.2020, 05.06.2020 Paolo Paioni | 17.05.2020 Beat Bangerter | 22.05.2020 Vera Jäggi | 20.04.2020, 16.05.2020, 22.05.2020, 09.06.2020

4.3 The Acceptable Use Policy (AUP) of the Leonhard Med

https://rechtssammlung.sp.ethz.ch/Dokumente/438.1.pdf

4.4 Signing the Policies

SwissPK^cdw tenant and AUP of Leonhard Med User Personal Statement

By signing the document I declare that I have read, understood and agree with the "*SwissPK^cdw* User Policy" and "The Acceptable Use Policy of the Leonhard Med secure High Performance Computing Infrastructure" and will abide by them.

Name _____

Date _____

Signature _____