Scientific IT Services
IT Services, ETH Zurich

Data and Computing Services for Personalized Health Research

High Performance Computing for genomic applications

Dr. Diana Coman Schmid
Service Manager, Personalized Health Data Services
Scientific IT Services, ETH Zurich

Outline

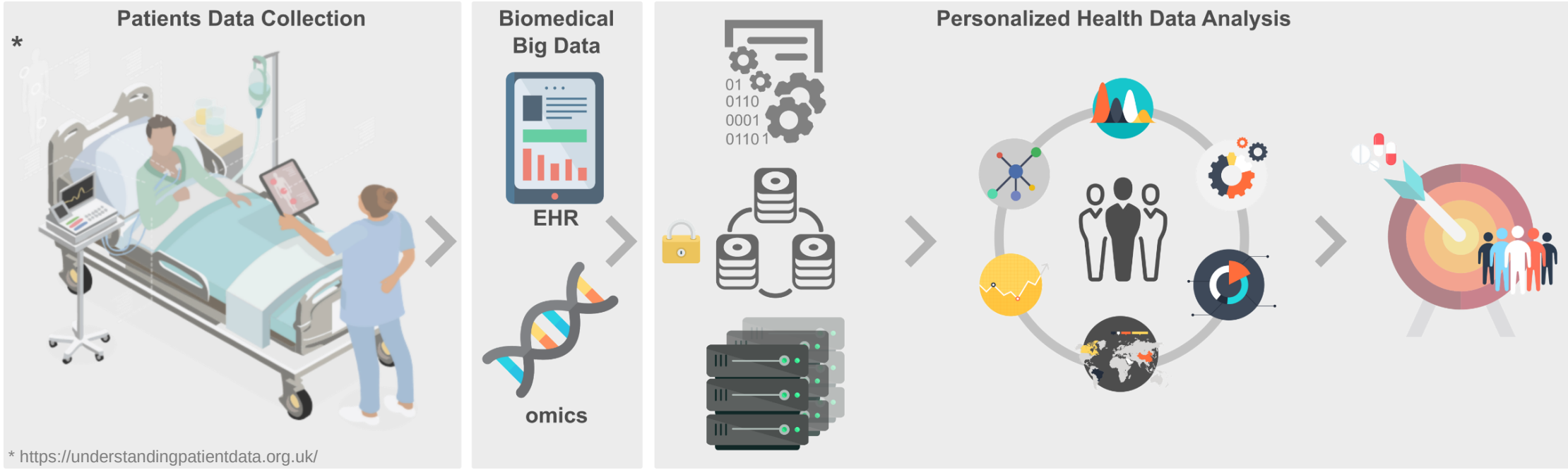
- personalized health (PH) research: data driven, sensitive personal data (confidential data)
- data confidentiality and individuals privacy in PH Research: data protection and IT security awareness
- secure data and computing services for PH research: Leonhard Med and BioMedIT

Personalized health (PH) research

Data driven, sensitive personal data (confidential data)

Personalized Health Research

Goal: provide the **right treatment**, at the **right moment** to the **right patients** (precision medicine) and ensure that as many people as possible **stay healthy** (prevention; personalized health).



Research on human data: sensitive personal data
Hereafter, per convention: confidential research data

Personalized Health Research

Trends

Confidential research data

Individual Studies

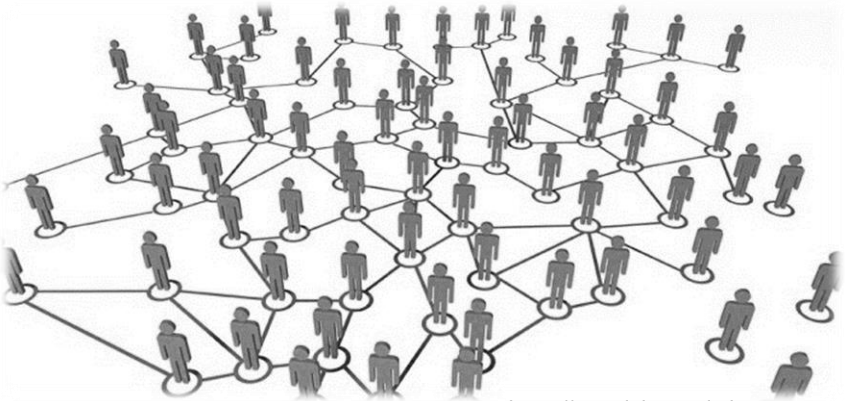
Classical Biomedical Research

Data Driven Biomedical Research

Now

Networks of Studies

Citizens



https://www.laboursolutions.com.au

Priv. Conf. Risk

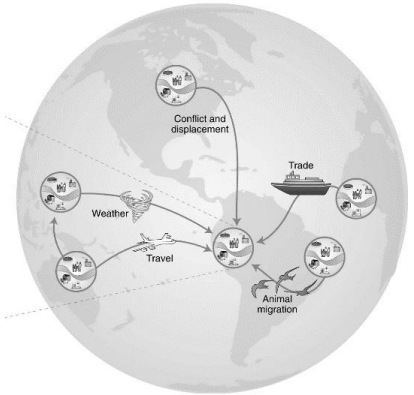
Data FAIRness

Datasets are combined

One Health

http://www.oie.int/en/for-the-media/onehealth/

Global Health



Hernando-Amado *et al.*, 2019, Collignon *et al.*, 2018

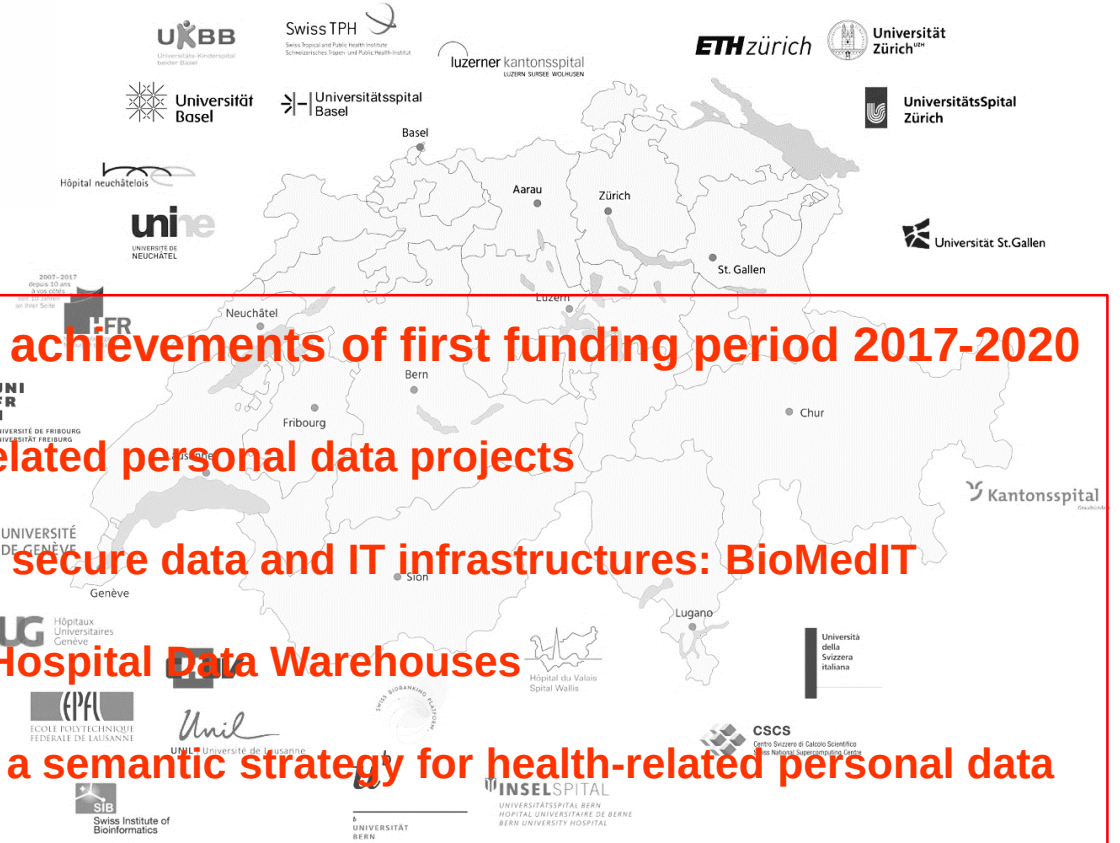
Swiss Programs for Personalized Health Research

2017 — 2020 — 2024

Swiss Personalized Health Network

THE LOOP ZURICH
MEDICAL RESEARCH CENTER

ETH
Strategic Focus Area
Personalized Health and Related Technologies



SPHN key achievements of first funding period 2017-2020

- **24 health-related personal data projects**
- **building up secure data and IT infrastructures: BioMedIT**
- **setting up Hospital Data Warehouses**
- **developing a semantic strategy for health-related personal data**

https://www.sphn.ch/

Handling confidential data in research > a _____ Paradigm Shift

From

Standard Research Infrastructure and Services

Towards

Secure & Versatile & User-friendly Scientific Data and IT Services

PROTECT CONFIDENTIAL DATA & INDIVIDUALS PRIVACY WHILE DOING RESEARCH

Legal & Ethics

- Sensitive personal data
- Data types & legal specification, ethics
- Strictly controlled data access, use and sharing

Infrastructure & Services

- Distributed data providers and large data lakes
- Dataset combination: central vs. federation
- FAIRness of sensitive personal data
- Storage and compute power

Usage

- Researchers: security & usability
- Clinicians: UX, web services
- Citizens:

https://www.midata.coop MIDATA.coop

https://swissdatacustodian.ch Swiss Data Custodian

NEW ecosystem

Data confidentiality and individuals privacy in PH Research

Data protection and IT security awareness

Data > Personal and Confidential Data (Sensitive Personal Data)

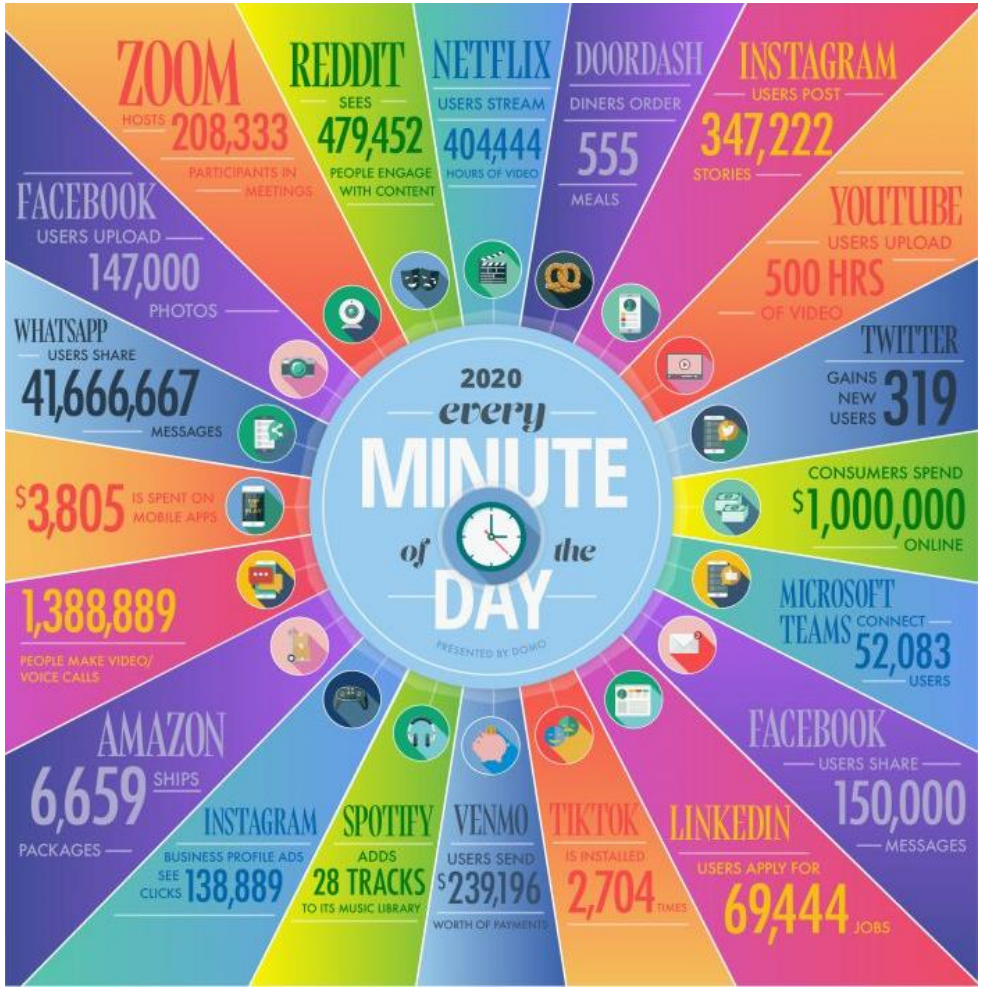
Data Privacy and IT Security Training

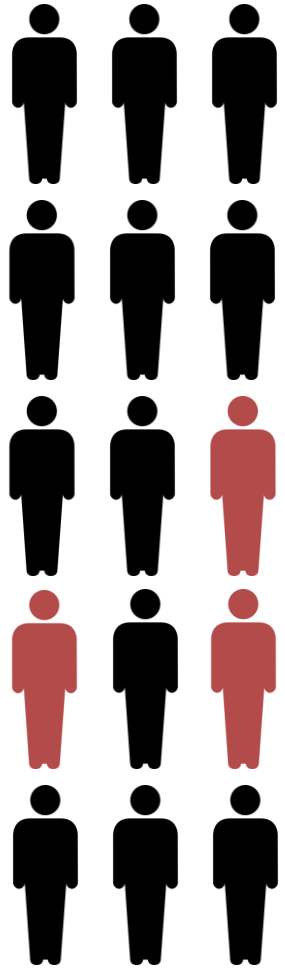
https://edu.sib.swiss/course/view.php?id=424

~ 2.5 quintillion
bytes of data
are created every day

90 % of all data
was produced in the last few years

50 TB of data
could easily be generated by a person every year





https://www.domo.com/learn/data-never-sleeps-8

Digital life > do you have control?

Data Privacy and IT Security Training

https://edu.sib.swiss/course/view.php?id=424

Terms of Service

reading

click & agree

https://www.dimayarovinsky.com/#/i-agree/

Where is my data

Who uses it

For what

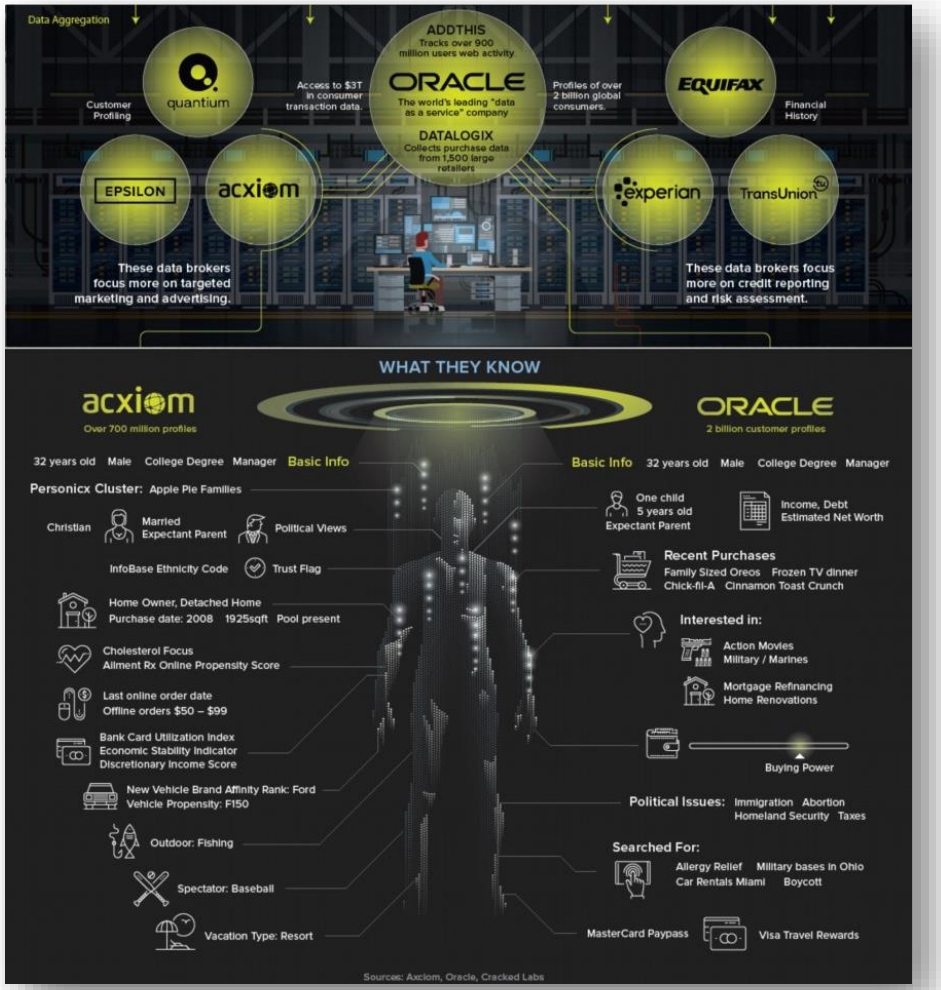
Digital life > do you have control?

Data Privacy and IT Security Training

https://edu.sib.swiss/course/view.php?id=424

2.7 billion

personal profiles stored



http://www.visualcapitalist.com/personal-data-ecosystem/

2-4 breaches

involving **medical data** every week (US)

October 27, 2020

Helsinki, Finland (CNN Business) **confidential records of thousands of psychotherapy patients** in Finland have been hacked and some are now facing the **threat of blackmail**. Attackers were able to steal records related to **therapy sessions, as well as patients' personal information**

https://edition.cnn.com/2020/10/27/tech/finland-therapy-patients-blackmailed-data-breach-intl/index.html

Personal Data for Research > examples

Data Privacy and IT Security Training

https://edu.sib.swiss/course/view.php?id=424

In what area of your life would you like to increase your feelings of happiness? Select all that apply.

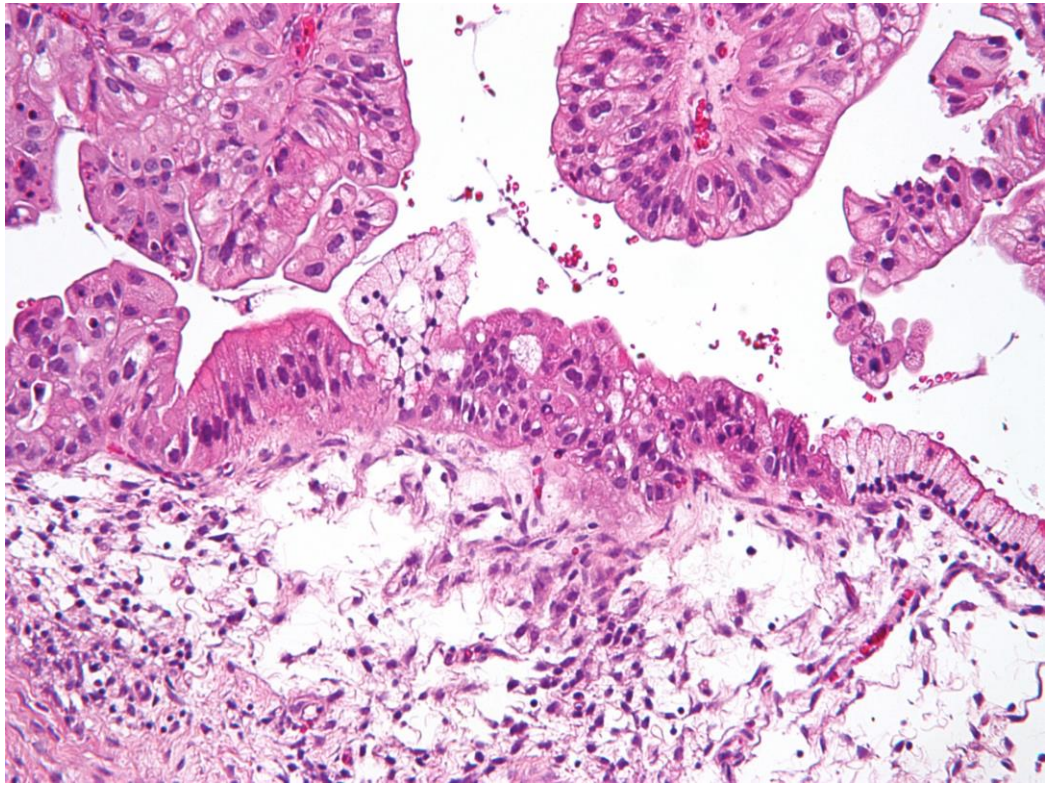
- [ ] Family
- [ ] Friends
- [ ] Relationship
- [ ] Workplace
- [ ] Career
- [ ] Health
- [ ] Wealth
- [ ] Surroundings
- [ ] Leisure time

Please state your agreement with the below statements:

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I am pleased with the way I am	○	○	○	○	○
I am pleased with the way I approach life	○	○	○	○	○
I am pleased with the way I approach problems	○	○	○	○	○
I am rarely interested in other people	○	○	○	○	○
I feel that life is rewarding	○	○	○	○	○
I am committed and involved	○	○	○	○	○
I always see the bad in people	○	○	○	○	○

https://www.questionpro.com/survey-templates/happiness-survey-template/

Happiness survey



https://upload.wikimedia.org/wikipedia/commons/thumb/b/b8/Mucinous_lmp_ovarian_tumour_intermed_mag.jpg/350px-Mucinous_lmp_ovarian_tumour_intermed_mag.jpg

Pathology image

Personal Data for Research > examples

Data Privacy and IT Security Training

https://edu.sib.swiss/course/view.php?id=424

- Personal data
- Sensitive (health-related); «happiness» data too?
- De-identified from Research perspective:
  - Whose pathology image this is ? No info
  - Who answered «Career» ? No info
- Qualitative, Quantitative Research:
  - ✓ What diagnosis based on pathology image
  - ✓ How many answered «Career»
- Data protection:
  - Sensitive personal data (health-related)
  - What is the risk for data confidentiality and individuals privacy ?

Personal Data for Research > examples

Data Privacy and IT Security Training

https://edu.sib.swiss/course/view.php?id=424

European Social Survey

Privacy Notice

How ESS collects your Information

When you register to access the ESS data we will collect data to allow us to record user details.

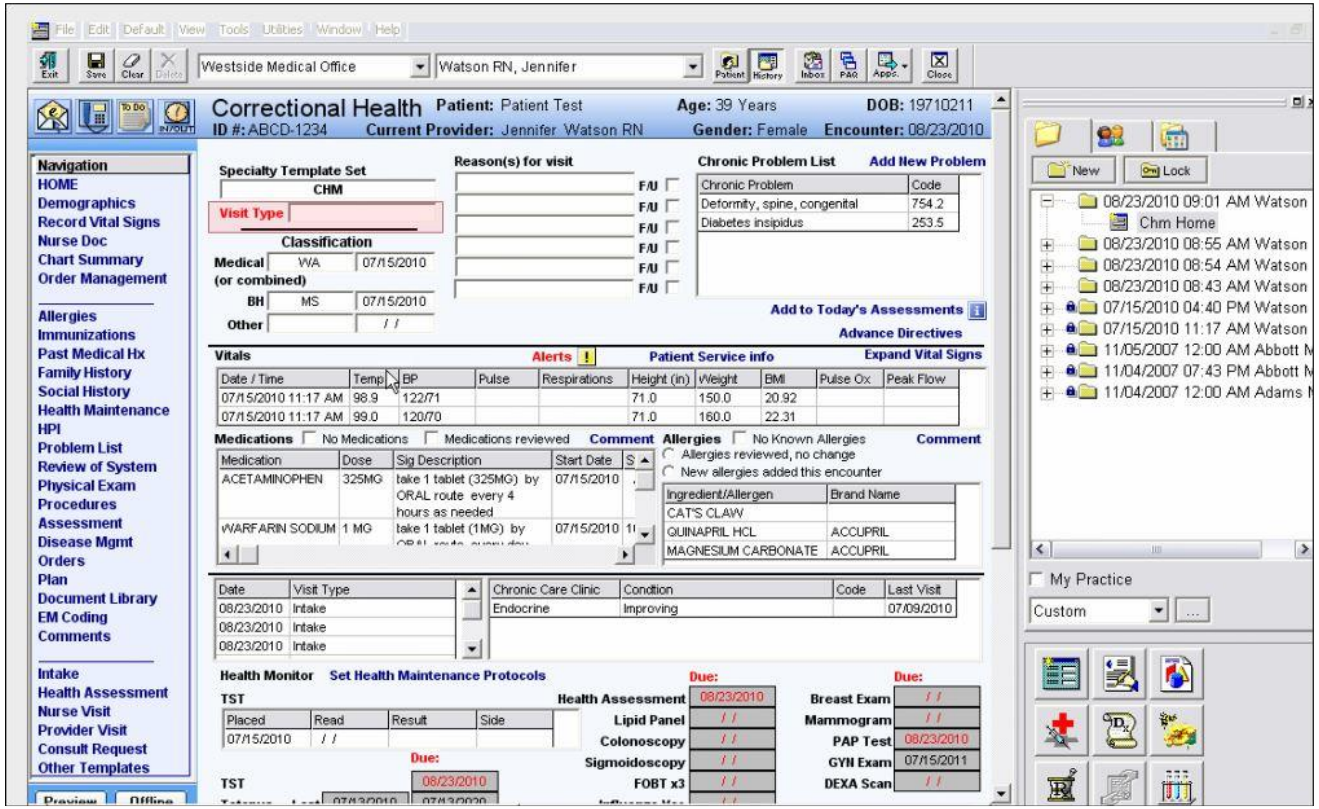
What Information ESS collects

ESS may collect the following types of personal data about you:

- Your name (title, first and surname) and contact information such as address, email address and institutional address. Your country of domicile and user category (eg Faculty member, PhD Student, Government official or other) as well as the academic discipline are recorded.
- The personal data are stored in a safe environment in accordance with GDPR requirements at NSD – Norwegian Centre for Research Data, Bergen, Norway. Backup systems are provided by the University of Bergen, Norway.

https://www.europeansocialsurvey.org/about/web_privacy.html

Social survey



Electronic Health Record

https://medrecordsinfo.com/healthfusion-stands-out-among-emr-software-solutions/

Personal Data for Research > examples

Data Privacy and IT Security Training

https://edu.sib.swiss/course/view.php?id=424

- Personal data
- Sensitive (health-related)
- Identifying information at Data Controller:
  - directly: name, address, etc.
  - indirectly: gender, age, medical history etc.
- Data protection:
  - Sensitive personal data (health-related) with identifying information
  - What is the risk for data confidentiality and individuals privacy ?

European Social Survey

How ESS collects

When you register to acce
user details.

What Information

ESS may collect the follow

- Your name (title, first a
  email address and insti
  (eg Faculty member, Ph
  academic discipline are
- The personal data are s
  requirements at NSD – Norwegian Centre for Research Data, Bergen, Norway.
  Backup systems are provided by the University of Bergen, Norway.

https://www.europeansocialsurvey.org/about/web_privacy.html

Social survey

Electronic Health Record

https://medrecordsinfo.com/healthfusion-stands-out-among-emr-software-solutions/

Research on confidential data > basic awareness

Data Privacy and IT Security Training

https://edu.sib.swiss/course/view.php?id=424

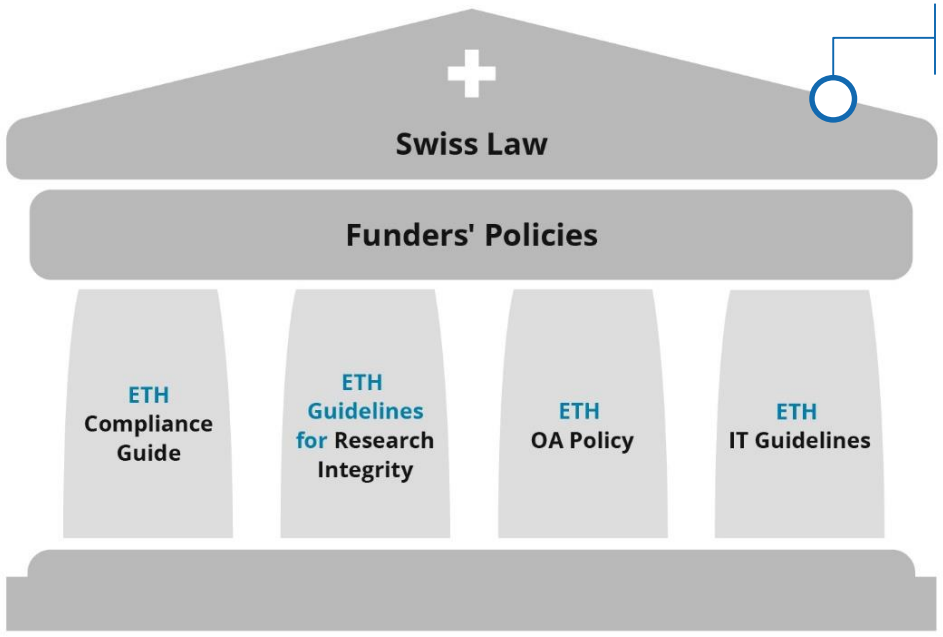
DMP	▪ Who “owns” persons/patients data, who and how “controls” these data ▪ Did the persons/patients give consent? ▪ Are the data de-identified, anonymized?	**Data governance**
ARDM ANALISYS	▪ Can my colleague send me briefly per encrypted e-mail a small dataset with data for only 5 patients for “quick” preliminary analyses? ▪ Can I use my laptop for “quick” look at this small dataset for the 5 patients? ▪ Can I send back to my research colleague preliminary findings about each of the 5 patients (patient level)? ▪ Do I need to keep track of who accessed/modified/deleted persons/patients data?	**Data transfer, use**
PUB.	▪ Am I allowed to publish persons/patients data in scientific journals? ▪ What happens if I publish patient data on open access research repos? ▪ What is the impact of data breach for myself, university, patients?	**Responsibility, accountability**

Research on confidential data requires special security measures: protect individuals privacy and ensure confidentiality of data OVER THE FULL DATA LIFECYCLE

Laws in Switzerland > Research, Human Data

Confidential Research Data

Sensitive Personal Data,



Adapted based on: Matthias Töwe
http://www.library.ethz.ch/en/Services/Courses-and-guided-tours/Workshops

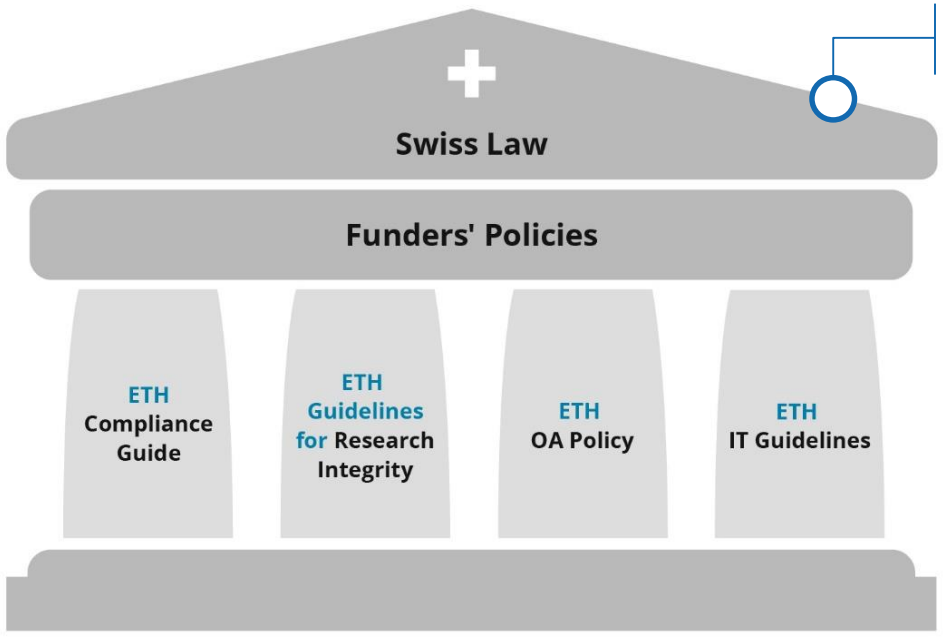
Swiss Criminal Code

Art. 321 Breach of Professional Confidentiality (rel. HRA)

Laws in Switzerland > Research, Human Data

Confidential Research Data

Sensitive Personal Data, *FADP Art. 3c*



Adapted based on: Matthias Töwe
http://www.library.ethz.ch/en/Services/Courses-and-guided-tours/Workshops

Federal Act on Data Protection
Art. 3c Sensitive Personal Data

Human Research Act
Art. 32-35 Further Use of Biol. Material and Health-Related Pers. Data for Research

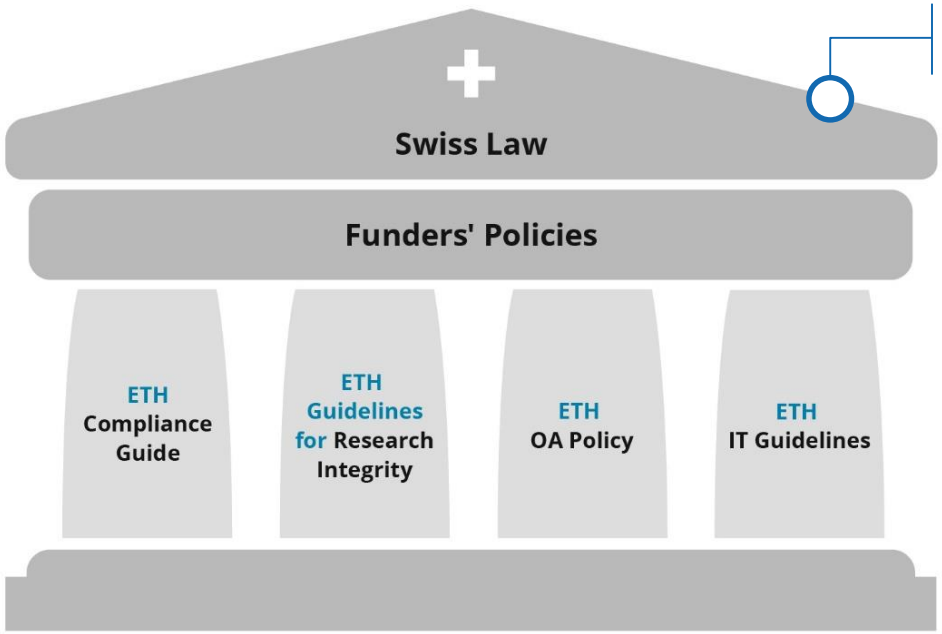
Human Research Ordinance
Art. 25-27 Anonymization, Coding
Art. 28-31 Informed Consent

Swiss Criminal Code
Art. 321 Breach of Professional Confidentiality (rel. HRA)

Laws in Switzerland > Research, Human Data

Confidential Research Data

Sensitive Personal Data, *FADP Art. 3c*



Adapted based on: Matthias Töwe
http://www.library.ethz.ch/en/Services/Courses-and-guided-tours/Workshops

Federal Act on Data Protection

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Art. 3c Sensitive Personal Data

The following definitions apply:

a. *personal data (data):* all information relating to an identified or identifiable person;
b. *data subjects:* natural or legal persons whose data is processed;
c. *sensitive personal data:* data on:
   1. religious, ideological, political or trade union-related views or activities,
   2. health, the intimate sphere or the racial origin,

e. *processing:* any operation with personal data, irrespective of the

Examples of personal data

Data Privacy and IT Security Training

https://edu.sib.swiss/course/view.php?id=424

Directly identifying information

- Full name & home address
- ID number
- Driver licence
- Social security number
- Biometric information (incl. finger prints)
- Genetic information

Indirectly identifying information

- Gender
- Birth date
- Job position
- IP address
- Blood sugar levels
- Daily movements

Examples of personal data

Data Privacy and IT Security Training

https://edu.sib.swiss/course/view.php?id=424

Directly identifying information

- Full name & home address
- ID number
- Driver licence
- Social security number
- Biometric information (incl. finger prints)
- Genetic information

Sensitive Personal Data

Indirectly identifying information

- Gender
- Birth date
- Job position
- IP address
- Blood sugar levels
- Daily movements

Personal Data

Examples of personal data

Data Privacy and IT Security Training

https://edu.sib.swiss/course/view.php?id=424

Directly identifying information

- Full name & home address
- ID number
- Driver licence
- Social security number
- Biometric information (incl. finger prints)
- Genetic information

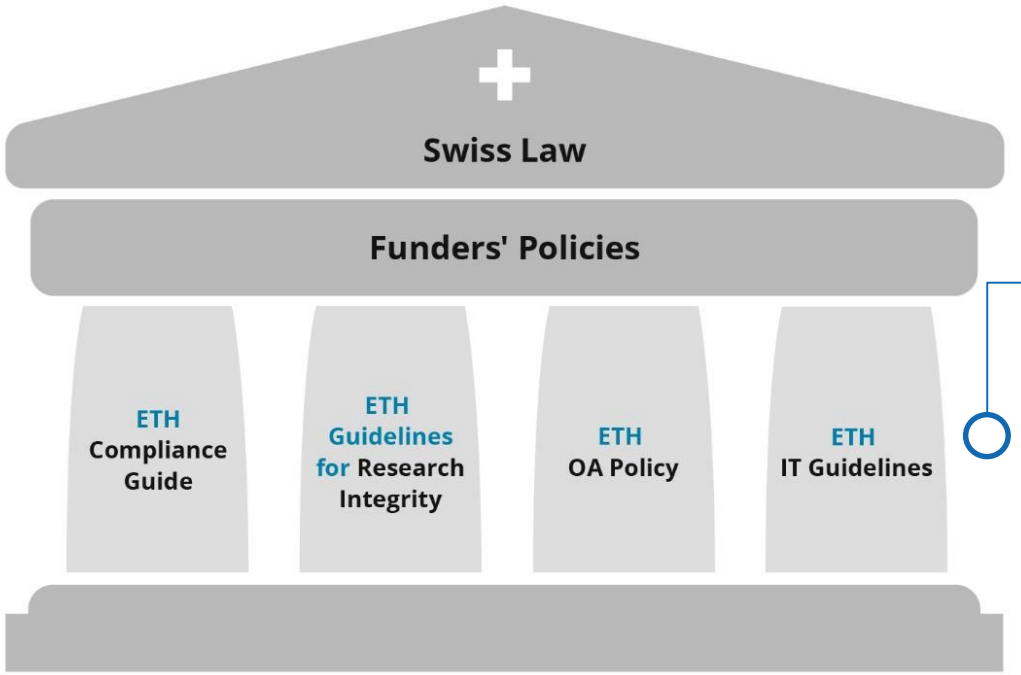
Sensitive Personal Data

Indirectly identifying information

- Gender
- Birth date
- Job position
- IP address
- Blood sugar levels
- Daily movements

Personal Data

Research Regulations > Research, Human Data



ETH [see RDM S1, 2, 6]

- Compliance Guide
- Guidelines for Research Integrity
- Open Access Policy

ETH IT Policies

- Directive on Information Security
- Acceptable Use Policy for Telem. Res. (BOT)
- Leonhard Med Acceptable Use Policy
- Leonhard Med Endpoints

National level, EU

- SPHN Information Security Policy
- SPHN ELSI Framework
- Good Clinical Practice, GCP ICH E6(R2) https://www.ema.europa.eu
- *See GDPR*

IT Security Guidelines ETH > Research

The following information describes IT-security related documents and guidelines, which apply to the employees of ETH Zurich.

Open all +

Acceptable Use Policy for Telematics Resources	Open +
Information Security	Open +
Standards System Care	Open +
Best Practice Rules	Open +
Web Policy	Open +
Software Licenses Guidelines	Open +
Leonhard Med	Open +
Internal information	Open +

General

Specific to Confidential Data

IT Security Guidelines ETH > Research, Human Data

The following information describes IT-security related documents and guidelines, which apply to the employees of ETH Zurich.

Open all +

Leonhard Med Open +

Specific to Confidential Data

Effective May 2019

Acceptable Use Policy

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

Scope:
prevent breach of confidentiality, integrity, or availability of […] Data entrusted to the "Leonhard Med IT" system.
Roles & Definitions:
Project Leader, User, Confidential Data
PL: *accountable* whole project data life cycle in LeoMed
Compliance: must be signed by every User

Guidelines for ETH Zurich LeoMed Endpoints

https://rechtssammlung.sp.ethz.ch/Dokumente/438.2.pdf

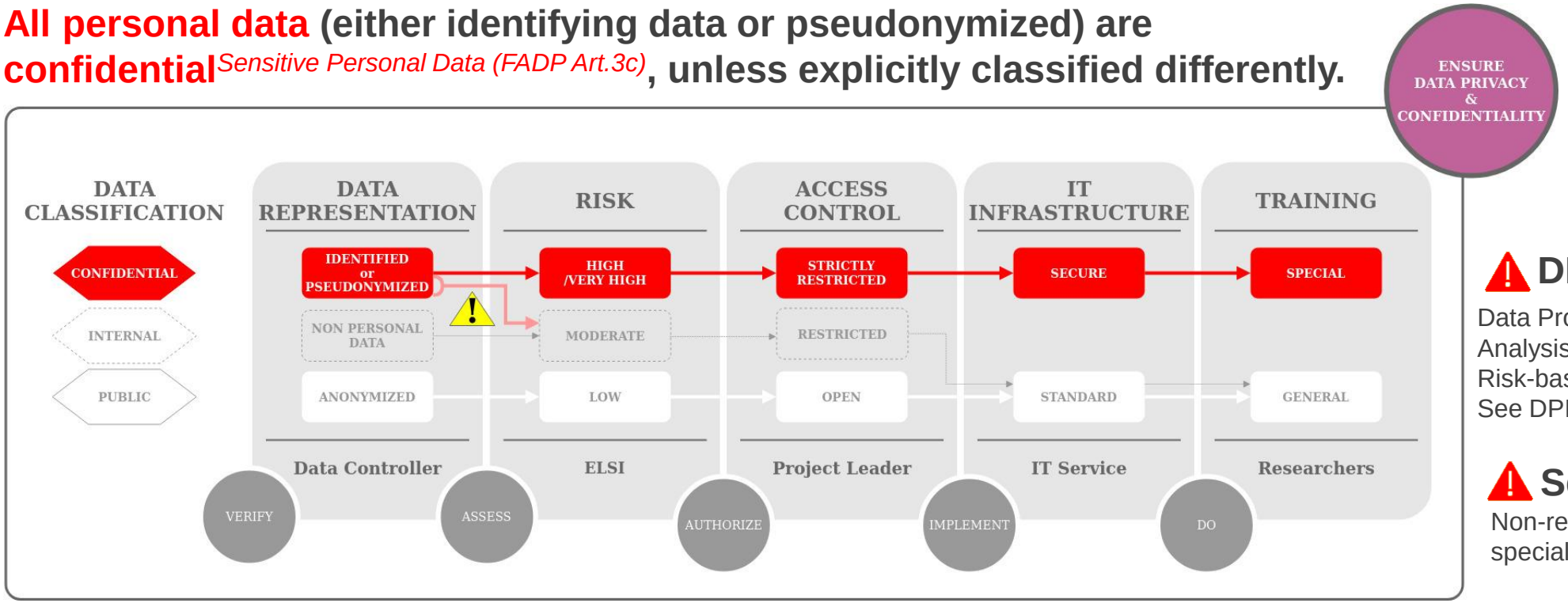
Scope:
requirements for the secure setup, maintenance and use of computer systems […] “Endpoint” to Leonhard Med
Roles & Definitions:
Project Leader, User, Endpoint
PL: *accountable*, User: *responsible* for Endpoint security
Compliance: mandatory […] for members of ETH Zurich

Data classification

YES or NO: **Confidential Research Data** compliant with Swiss legislation and policies

Data classification policy: Leonhard Med, ETH and SPHN *Swiss Personalized Health Network*

All personal data (either identifying data or pseudonymized) are confidential *Sensitive Personal Data (FADP Art.3c)*, **unless explicitly classified differently.**



DPIA

Data Protection Impact Analysis
Risk-based
See DPIA at ETHZ

Secret Data

Non-research / very special research projects

Data classification scenarios <>Technical & Organizational Measures

Data classification guidelines

Confidential Research Data

Genotyping data (DNA sequencing)

- WGS (Whole Genome Sequencing) data
- WES (Whole Exome Sequencing) data
- Specialized genomic panels (e.g. cancer panels)
- Single cell sequencing, ChIP-seq, ATAC-seq
- Information in some types of QC files

Examples: the content of

- Raw sequence reads in **FASTA** or similar formats
- **VCF** (Variant Calling Format)
- **SAM** (Sequence Alignment/Map) and **BAM** (binary version of SAM)

Data classification guidelines

Data Privacy and IT Security Training

https://edu.sib.swiss/course/view.php?id=424

Confidential Research Data

- **Raw data** in genomics, transcriptomics, proteomics
- Patient derived human cell lines
- Biobanks and cohorts
- Imaging data
- Immunological screening
- Controlled access data in TCGA, dbGAP

- *Note: data in combined datasets (aggregation) are often confidential*

For now, these are **strictly guidelines** (i.e. defined per policy and not defined in laws to this level of detail)

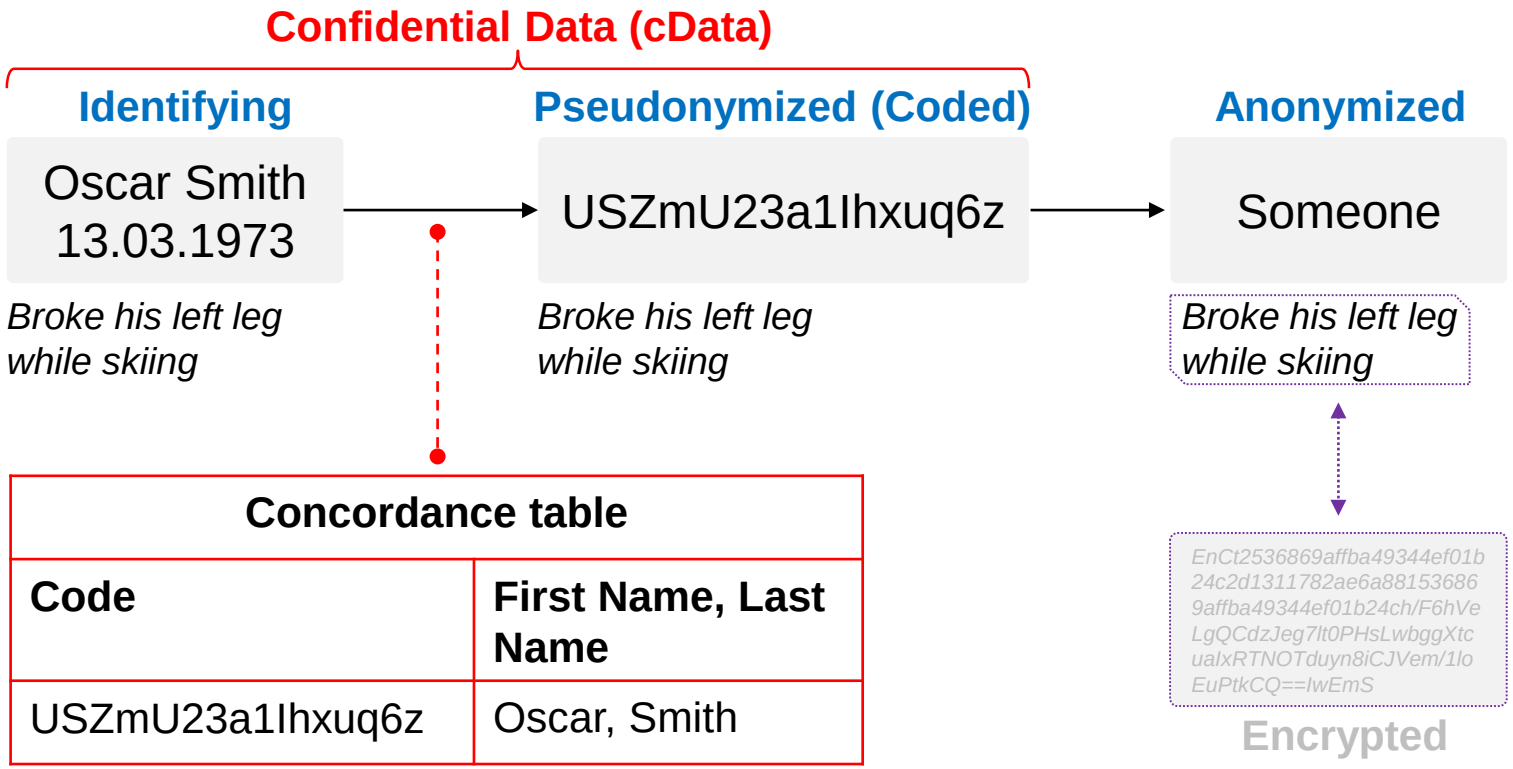
Confidential Data > a Representation Example

Data Privacy and IT Security Training

https://edu.sib.swiss/course/view.php?id=424

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

A Guide for technical and organizational measures
The Federal Data Protection and Information Commissioner (FDPIC) 2015

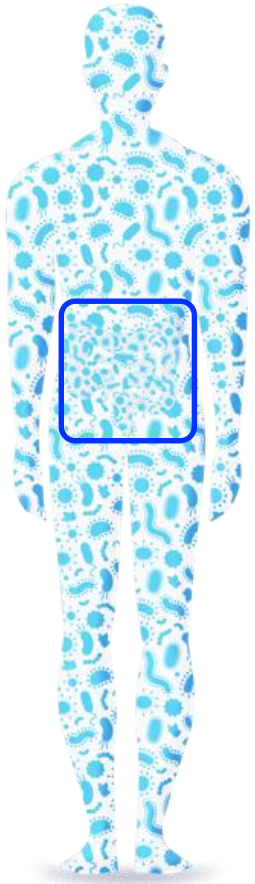


- **IF concordance table exists, data are NOT anonymous**
- **Pseudonymization: identifying information is replaced by a code (e.g. concordance table) only accessible with a "key" under strict security regulations**
- **⚠ Pseudonymized data are confidential data**

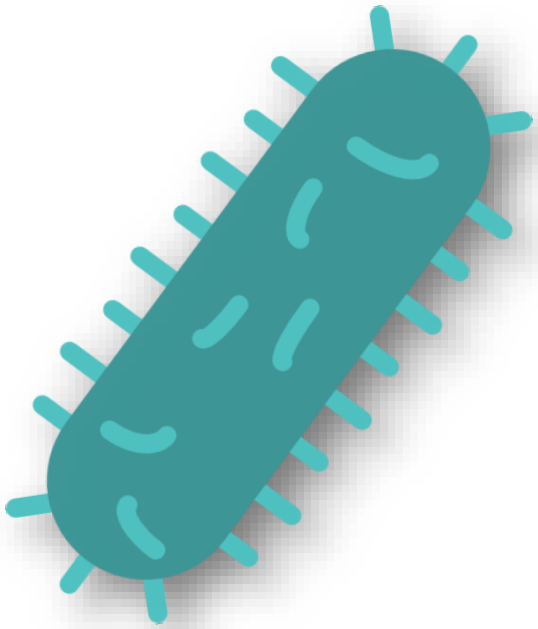
Research Data Classification *per policy* > Confidential ¦ Public ¦ Internal

Genome
Health records
Some social surveys
Psychiatry video sessions
Mobility profiles
...

⚠ **Microbiome**
- sampled from human
- may identify people*



https://www.viome.com/our-science



Bacteria
- sampled from hospital
- non-human data
- near real-time surveillance

* Franzosa et al., 2015, Wagner et al., 2016

Confidential + Public = Confidential

Anonymisation, HRO (art. 25)

For the anonymisation of biological material and health-related personal data, **all items which, when combined, would enable the data subject to be identified without disproportionate effort, must be irreversibly masked or deleted**.
In particular, the name, address, date of birth and unique identification numbers must be masked or deleted.

Anonymized data are out of HRA scope

Confidential Data terminology

Data Privacy and IT Security Training

https://edu.sib.swiss/course/view.php?id=424

- **de-identification:** process used to prevent a person's identity from being connected with information, i.e., the identity of a person can't be obtained anymore
  - **Pseudonymization = coding**: substitutes the identity of a data subject in such a way that additional information is required to *re-identify* the data subject. For example, name, age and home address are substituted by a unique code.
  - **anonymization:** irreversibly destroys any way of identifying a data subject. *Note: anonymization must not be confused with pseudonymization!*
- **re-identification**: process of matching de-identified data with publicly available information, or auxiliary data, in order to discover the individual to which the data belongs to.

Encryption: *processes of encoding a message (cf. SPHN Glossary)*

SPHN Glossary: https://www.sphn.ch/en/news-events-publications/publications.html

Summary > Data Privacy and Protection, Laws and Regulations

- Follow Swiss laws and regulations for using **confidential data** (i.e., sensitive personal data) in research
- Follow local, national , international applicable IT Security Policies and Guidelines
- Be aware of Roles (Project Leader, User, Data Processor etc.) and their Responsibilities and Accountabilities (e.g. data classification, data management etc.)
- Note the diff.: anonymized vs. coded/pseudonymized data
- Know that research with **confidential** requires TOMs (technical and organizational measures) **e.g. Secure Data and IT infrastructures**

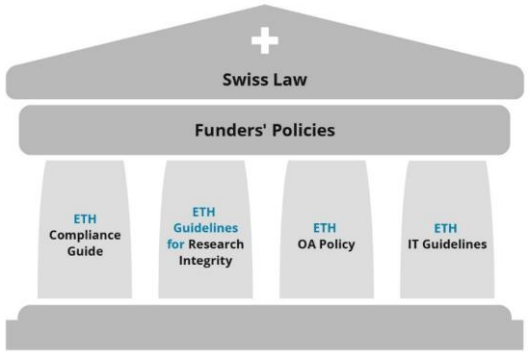
Secure data and computing services for PH research

Leonhard Med and BioMedIT

Laws and Regulations in Switzerland > Research, Human Data

Do researchers need to use special secure IT infrastructures?

Yes, if handling **CONFIDENTIAL DATA** *SENSITIVE PERSONAL DATA (FADP)* for research



Adapted based on: Matthias Töwe
http://www.library.ethz.ch/en/Services/Courses-and-guided-tours/Workshops

Secure scientific data & IT infrastructure

Technical & Organizational Measures

Leonhard Med

OR / AND

infrastructures with similar level of security*

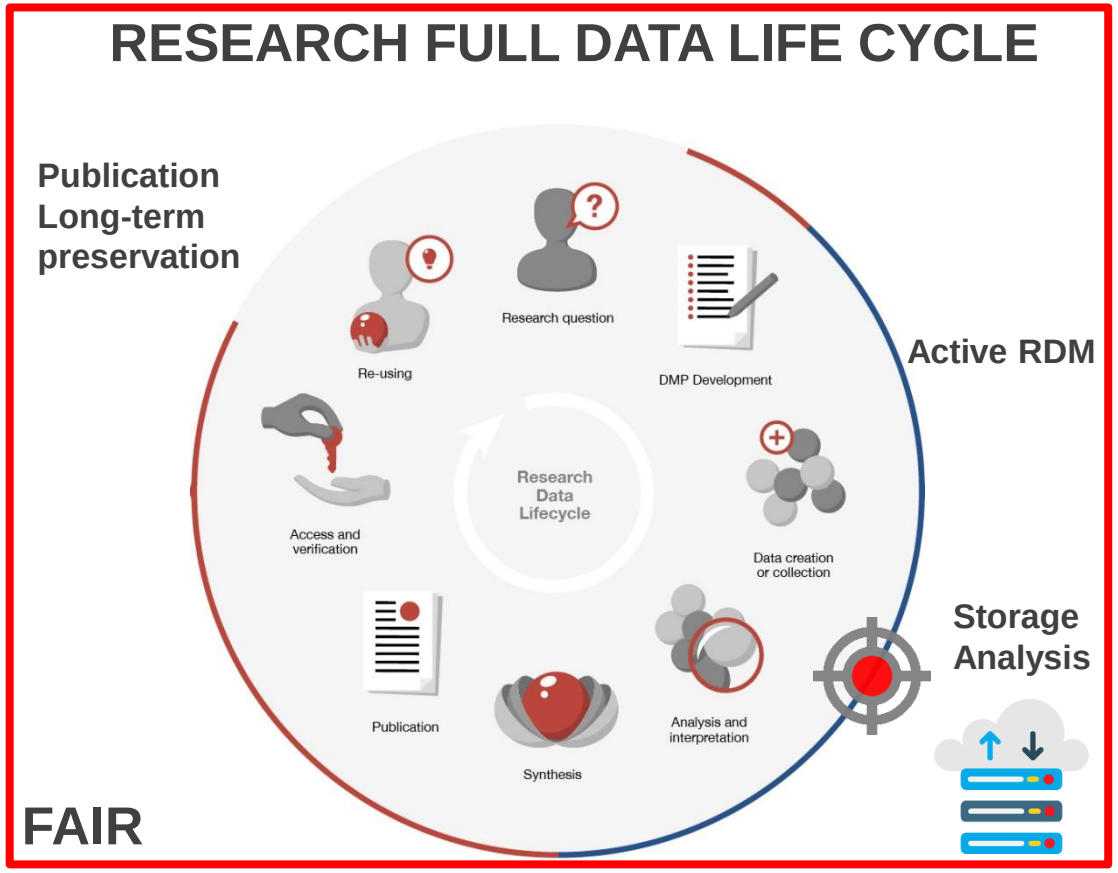
**consult your local IT support*

Secure handling of confidential research data - Technical & Organizational Measures (TOM)

Regulations for confidential research data

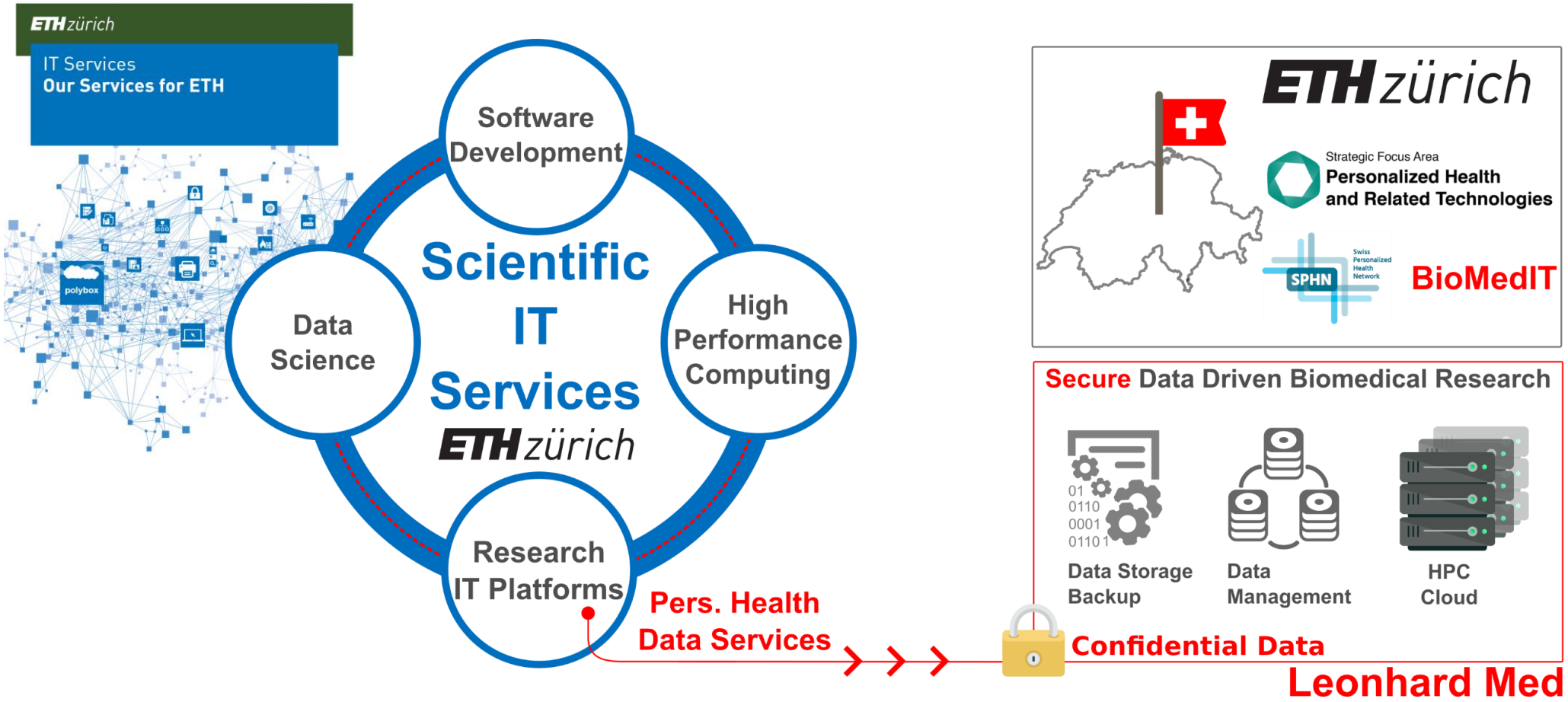
- Study participant **informed consent**
- **Ethical approval** to make data available for reuse in research
- **Contract** for data transfer from controllers (e.g. Hospitals) to secure Data & IT infrastructures (processors) where Researchers analyze data
- **Users** (e.g. researchers) are *Responsible to* comply with applicable regulations
- **Project Leaders** (e.g. PIs) are *Accountable* for the research Data Management over the full data life cycle
- **Secure Data and IT infrastructures** (data processor)

Secure scientific data & IT infrastructure



Technical & Organizational Measures

Leonhard Med: secure scientific data & IT platform, Scientific IT Services at ETH Zurich



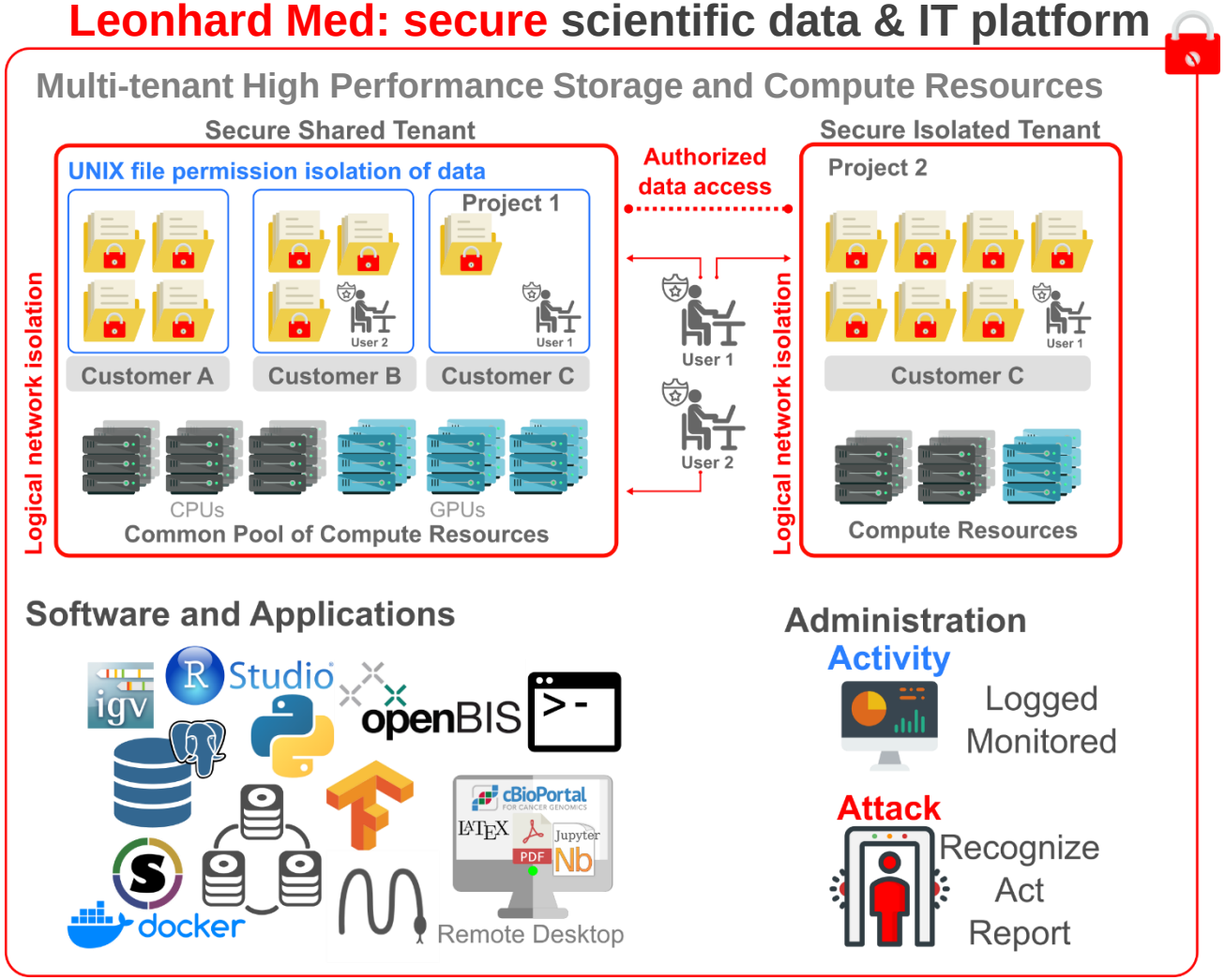
Leonhard Med: **secure** scientific data & IT platform for **bioinformatics** applications in data driven **biomedical research** and in general, for **confidential research data.**

Leonhard Med for ETH and Swiss Research with Confidential Data

Leonhard Med

- is a powerful research IT platform to securely store, manage and process (e.g. bioinformatics, data science) **confidential research data**
- enables collaborative, large-scale and very diverse **biomedical research** (including academies and hospitals) at ETH Zurich
- is part of the national **BioMedIT network** of secure data centers supporting projects in the SPHN and PHRT national programs

SPHN: Swiss Personalized Health Network
PHRT: Personalized Health and Related Technologies

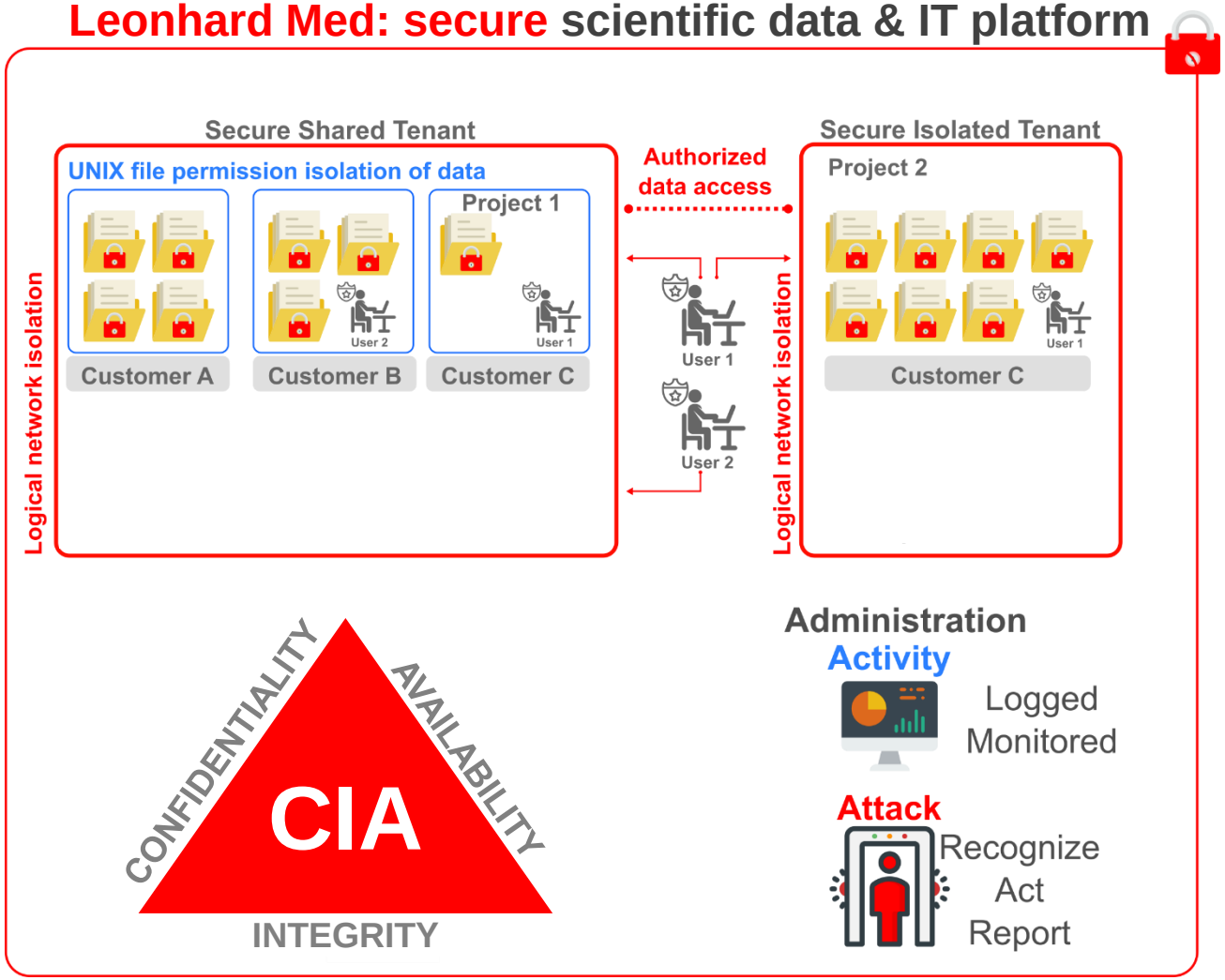


Technical & Organizational Measures

Leonhard Med security controls

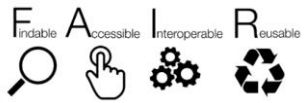
CIA measures, confidential data

- physical security of the data center
- data strictly isolated between customers
- user access strictly restricted
- internet access strictly controlled
- data encryption during transfer & in backup
- logging & monitoring
- Leonhard Med Acceptable Use Policy



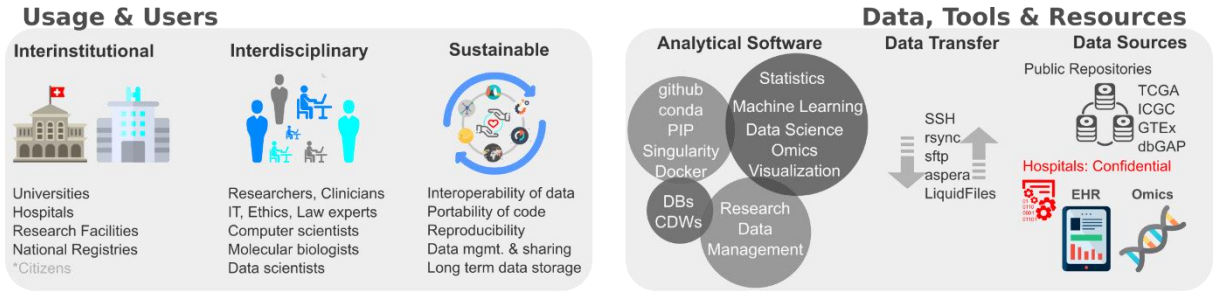
Technical & Organizational Measures

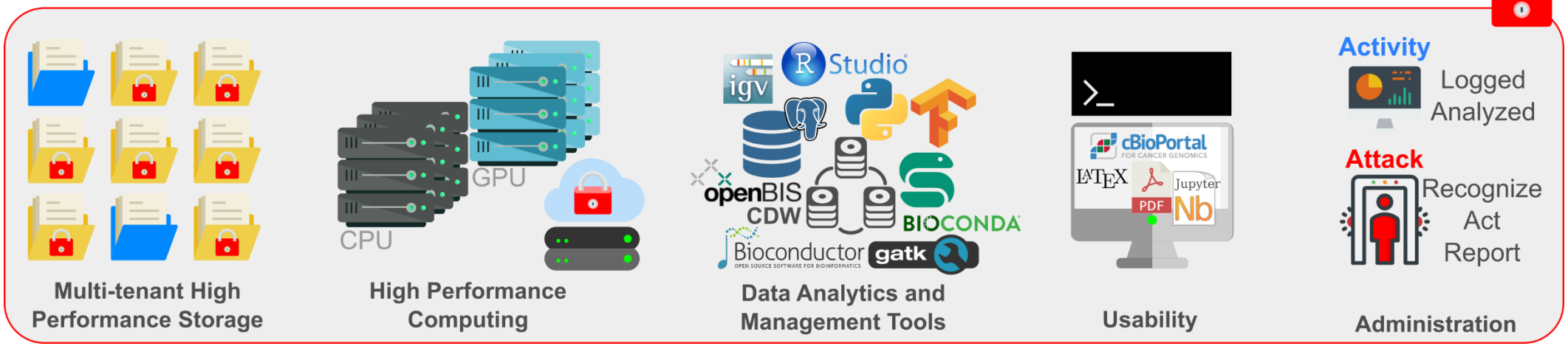
Leonhard Med as Bioinformatics Platform



Research Requirements

Leonhard Med





Leonhard Med: secure scientific data & IT platform

Leonhard Med data & IT platform: how can it be used for research?

- ☑ secure project space for data storage, management and analysis
- ☑ secure and collaborative compute environment for data analysis (bioinformatics, ML, etc.)
- ☑ secure data transfer from distributed sources
- ▶ customizable e.g., hosting specialized web-based applications, DBs, clinical data warehouses etc.

Leonhard Med: secure scientific data & IT platform

What are the rules and regulations of Leonhard Med?

Leonhard Med Acceptable Use Policy

Leonhard Med AUP

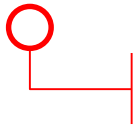
- ☑ **Project Leader (e.g. one of the PIs of a consortium)**
- ☑ **PL is accountable for the full data life cycle, including data classification***
- ☑ **Users are authorized to access and process project's data by PL**
- ☑ **PL and Every User must comply with the AUP**

** PL + Affiliated Legal Office* ▶ *DPIA* ▶ *Data Classification*

Data Protection Impact Analysis

Leonhard Med: secure scientific data & IT platform

How do I get to use Leonhard Med?



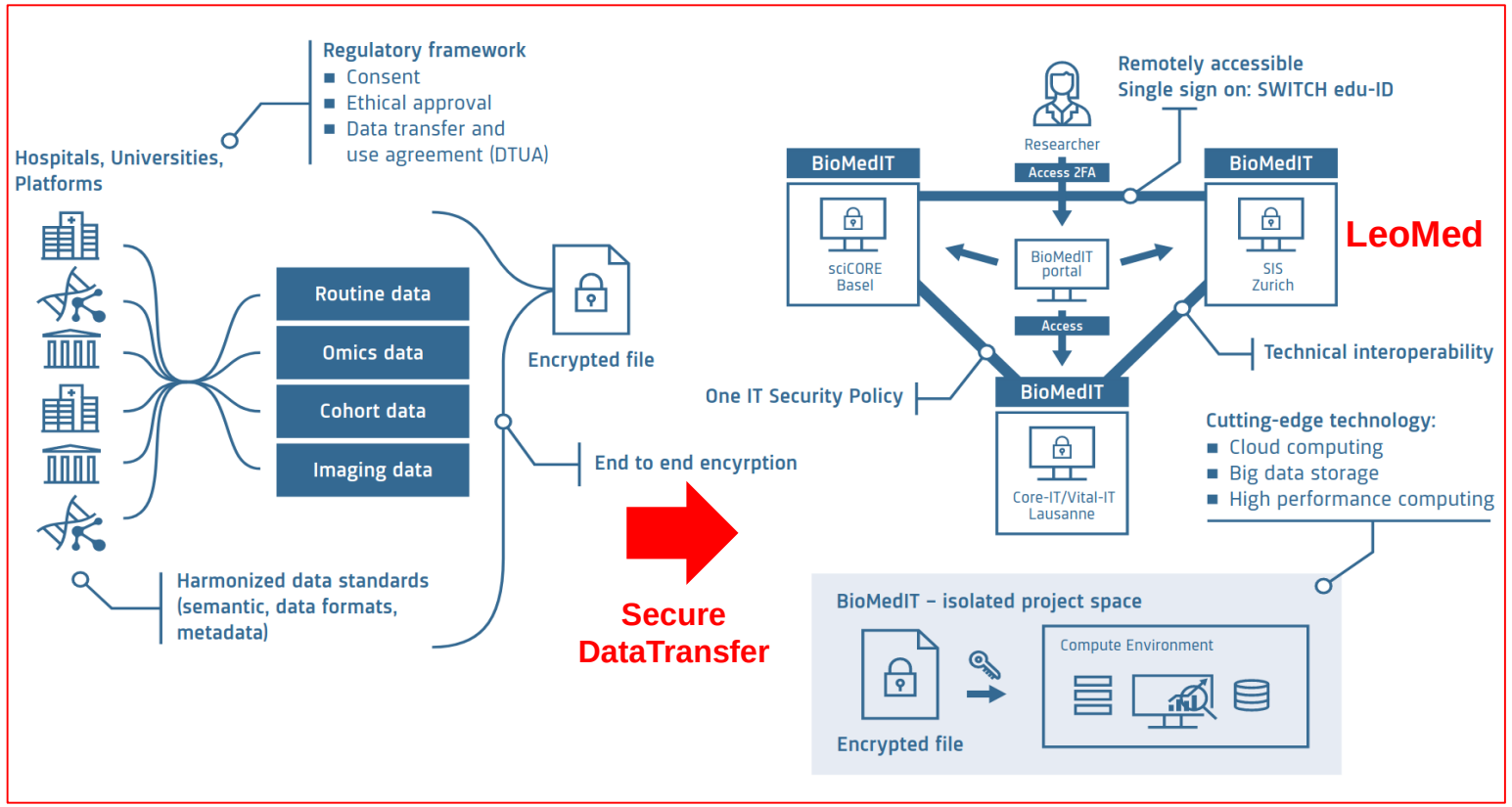
Leonhard Med information on service, regulations and expert consulting

Leonhard Med get in touch

- **Scientific IT Services, ETH Zurich and services for confidential data**
  https://sis.id.ethz.ch/services/index.html#confidential-research-data
- **Leonhard Med Service Level Agreement**
  https://ethz.ch/services/en/it-services/catalogue/server-cluster/hpc.html
- **Leonhard Med Acceptable Use Policy**
  https://rechtssammlung.sp.ethz.ch/Dokumente/438.1.pdf
- **Leonhard Med, support letter, budget, DMP etc.: contact diana.coman@id.ethz.ch**

Leonhard Med: the Zurich regional node of BioMedIT

Lowering computational boundaries for research with confidential data



- Data governance
- Secure data transfer process
- Data mgmt., data FAIRness
- Restricted data sharing (secondary use)
- Interoperability of data and bioinformatics workflows
- Data Privacy & IT Security Training

Adapted from: https://www.sphn.ch/

Sarah, Cancer Researcher using BioMedIT network

1 The **data query**: in order to build her research project, Sarah channels a data query via a Data Coordination Centre (DCC). She learns that three Swiss hospitals have patient data relevant to her project.

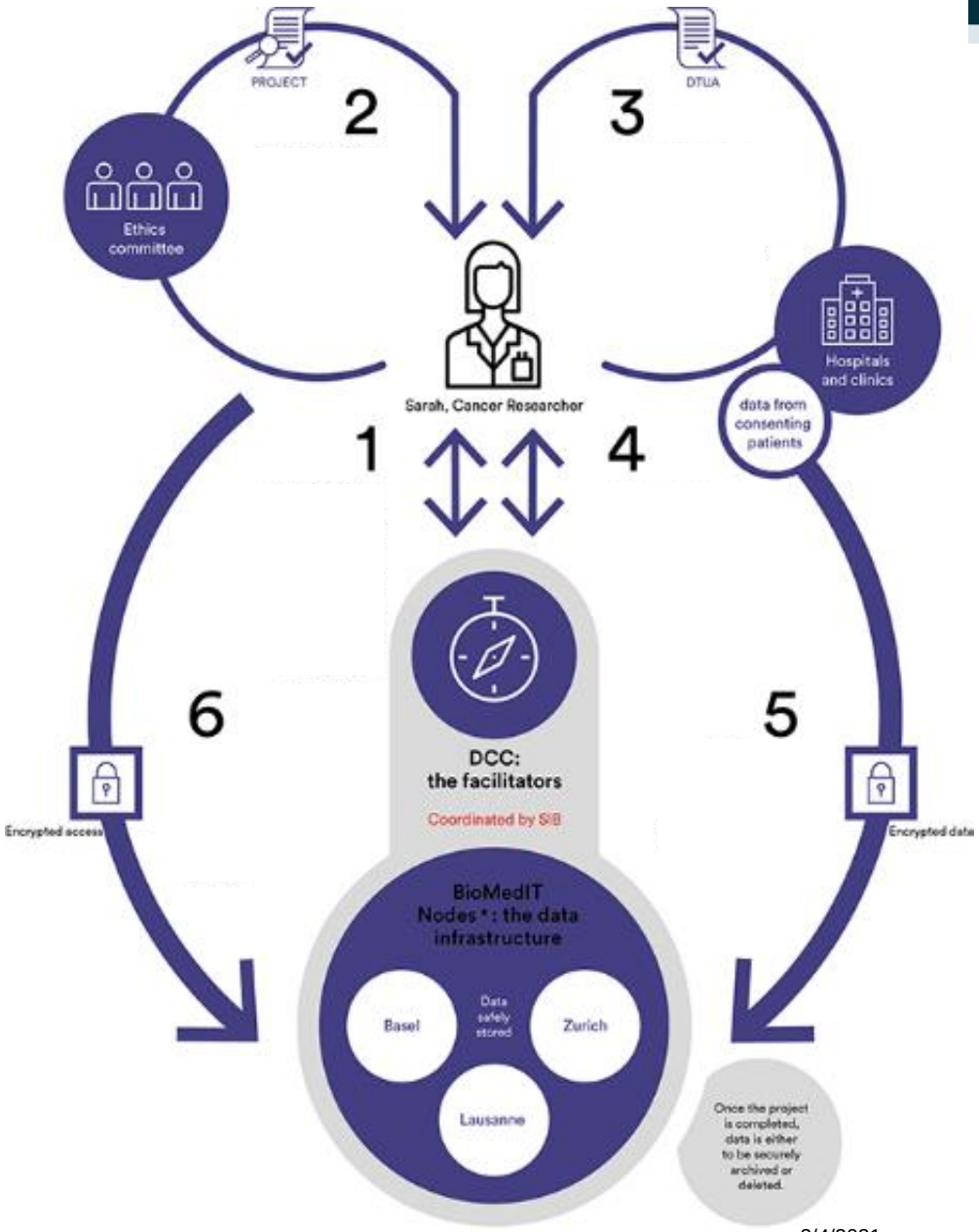
2 Obtaining **ethical clearance**: Sarah submits her project proposal, detailing the type and proposed usage of patient data, to an ethics committee, and obtains ethical approval.

3 Signing a **Data Transfer and Use Agreement (DTUA)**: Sarah requests data from the hospitals and signs a DTUA with the hospitals to formalize the data use rights and possible Intellectual Property derived from the research.

4 **Access rights** (and project registering) : Sarah registers the project and members of the research team at appropriate organization and obtains access rights.

5 **Secure data: handling**: The hospitals **encrypt** the **de-identified and consented patient data** and copy them to a secure research IT infrastructure for storage and processing (e.g. **Leonhard Med BioMedIT** node Zurich)

6 **Secure access and processing**: Sarah can now access the protected data at **Leonhard Med BioMedIT** node Zurich, do ARDM run her data analysis to proceed with her research project.



Best practices

Guidelines for secure handling of confidential research data over the full data life cycle

Best practices for secure handling of confidential research data

Do

- Know which data are confidential and which access restriction rules apply (i.e., as per DTUA)
- Aim for FAIRness of confidential research data *(note: FAIR data may be under restricted access; code & analytic methods under open access)*
- Be “security aware” (i.e., secure your computer) and follow relevant trainings (e.g. SPHN/BioMedIT, https://edu.sib.swiss/course/view.php?id=424)
- Follow data privacy rules (laws, policies, guidelines) and only handle confidential research data for which you have explicit authorization (i.e., by a Project Leader)
- Use TOMs over the full data life cycle, e.g., secure Data and IT infrastructures, data mgmt. plan, long term preservation etc.)
- Report promptly security incidents to responsible persons at your institution

Best practices for secure handling of confidential research data

Don't

- Don't work with data if you don't have explicit authorization, in doubt ask your research supervisor
- Don't share your login account used to access secure systems
- Don't copy confidential research data on your computer without authorization (i.e., by PL)
- Don't send confidential research data per regular e-mail or tools like regular Dropbox
- Don't share confidential research data for which you have use authorization without PL's permission
- Don't consider without formal confirmation (i.e., at Data Provider) that coded/pseudonymized data are anonymized and thus non-confidential
- Don't publish confidential research data in public repositories (e.g. GitHub)

Best practices for secure handling of confidential research data

Incompliance with relevant policies >> consequences

- Revocation of access right to confidential research data
- Revocation of access right to respective secure Data and IT infrastructures (e.g. Leonhard Med)
- Sanctions at home institute, Project Leader is accountable
- Depending on impact (i.e., minor vs. major data breach, unintentional vs. criminal misuse) individual researcher is accountable
- Swiss penal code might be applied
- Research impact (institution reputation, restrict data access etc.)
- *Note: moral obligation towards the individuals who had consented to share their sensitive personal data for research*

Further links general data and IT security at ETH

Information & IT Security in Everyday Life

Online training

Our compliance training provides comprehensive information on current topics of information and IT security. Take a look at the trailer!

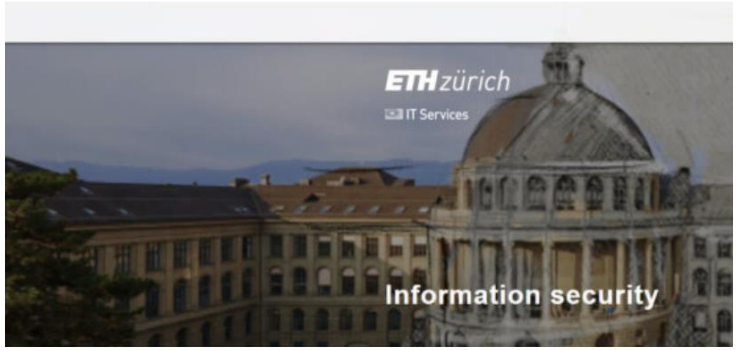
Everyday life topics

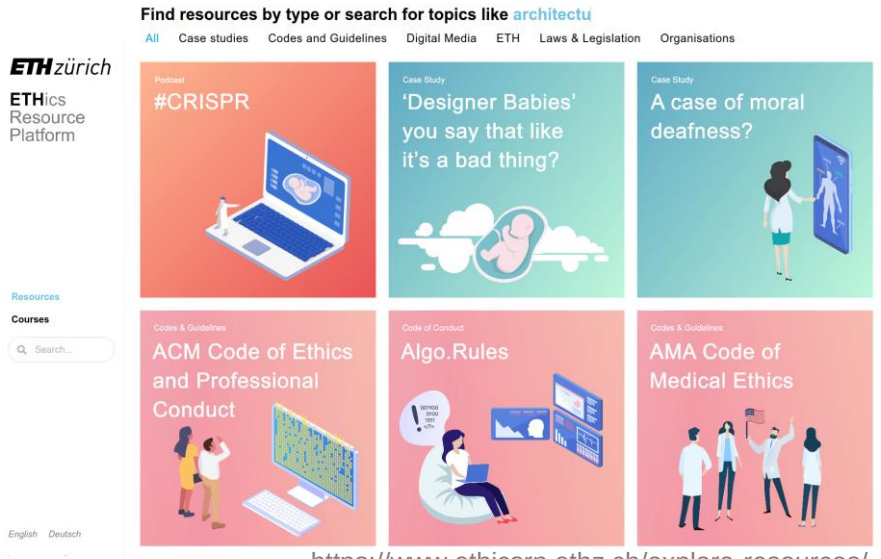
- Reporting Cyber Attacks & Incidents →
- Passwords, PINs, & Co. →
- Protecting Devices →
- Secure Handling of Email →
- Secure on the Internet →
- Social Engineering →
- Data Security →
- Information security house rules →

https://ethz.ch/services/en/it-services/it-security/awareness.html

https://blogs.ethz.ch/its/2019/12/18/compliance-training-information-security/#more-1902

"Information Security" training module





https://www.ethicsrp.ethz.ch/explore-resources/

Closing remarks

The 3 top things to think about your research & confidential data

Secure handling of confidential research data

The 3 top things to think about your research & confidential data

Data Confidentiality and Individuals Privacy Protection

- Data classification: e.g. public, internal OR confidential
  confidential research data requires strict protection
- Use TOMs for confidential research data in your research, e.g. Leonhard Med BioMedIT Node Zurich
  which laws and regulations, cybersecurity and data protection measures do you need to follow, what to do in case of data breach
- .. over the full data life cycle (FAIR). ⚠ Note: data analysis is «just» one of the steps in the process.

Thank you

for joining Data and Computing Services for Personalized Health Research

High Performance Computing for genomic applications

Dr. Diana Coman Schmid
Service Manager, Personalized Health Data Services
diana.coman@id.ethz.ch

ETH Zurich
Scientific IT Services
Binzmühlestrasse 130
8092 Zurich, Switzerland

https://sis.id.ethz.ch/

@ETH_SIS
@Diana_C_Schmid
@SPHN_ch
@PHRT_CH

Acknowledgements

- Michal Okoniewski, SIS ETHZ
- Leonhard Med Team and openBIS team, SIS ETHZ
- BioMedIT Team, SIB
- SPHN, PHRT partner projects