Responsible Data Sharing

Legal agreements for using health-related data in multi-center projects

Dr. Julia Maurer
Personalized Health Informatics Group
SIB Swiss Institute of Bioinformatics
dcc@sib.swiss

A project of

Multi-center research projects

What are the requirements for data usage for most of the research projects in Switzerland?

- ✓ Project plan
- ✓ Patients' consent
- ✓ Ethical approval/statement
- ✓ De-identified data (pseudonymized/coded)
- ✓ Technical security measures
- ✓ Legal agreement(s) among parties (Consortium Agreement/Data Transfer and Use Agreement)

Overview legal agreements for research purposes

- Consortium Agreement (CA)
- Data Transfer and Use Agreement (DTUA)
- Data Transfer and Processing Agreement (DTPA)

- Material Transfer Agreement (MTA)
- Service agreements (lab, software developers, etc)

Overview legal agreements for research purposes

- Consortium Agreement (CA)
- Data Transfer and Use Agreement (DTUA)
- Data Transfer and Processing Agreement (DTPA)

Templates available here

- Material Transfer Agreement (MTA)
- Service agreements (lab, software etc)

MTA Templates available here

History of harmonized legal agreements for sharing data

In March 2019 a Data Transfer and Use Agreement (DTUA) Version 1.0 was published, developed by the representatives of the Swiss University Hospitals and national key players of Swiss research community.

BUT: it did not include the processing role of the BioMedIT network to be used in SPHN funded projects.

– remaining aspects provided by some university hospitals such as
  - Minimal security requirements
  - Information and audits of security measures

DTUA Version 2.0 including a Data Transfer and Processing Agreement (DTPA) was released and published Nov 2020 on the SPHN webpage.

Consortium Agreement (CA)

Purpose: Regulates the general principles of collaboration between the research partners

- Principle of collaboration
- Principle of data usage
- Governance
- Financial aspects
- Confidentiality
- Intellectual property
- Publications

Parties involved: Principal investigators/ project partners' home institutions

Data Transfer and Use Agreement (DTUA)

Purpose: Regulates the conditions under which a "Provider" (e.g. a hospital) agrees to disclose personal data to a "Recipient" (e.g. a university).

Parties involved: Institutions required to use and share data for the project

Provider and Recipient who jointly determine the purpose and means of the processing within the framework of the research project are considered as "Joint Controllers“.

The BioMedIT network as service provider

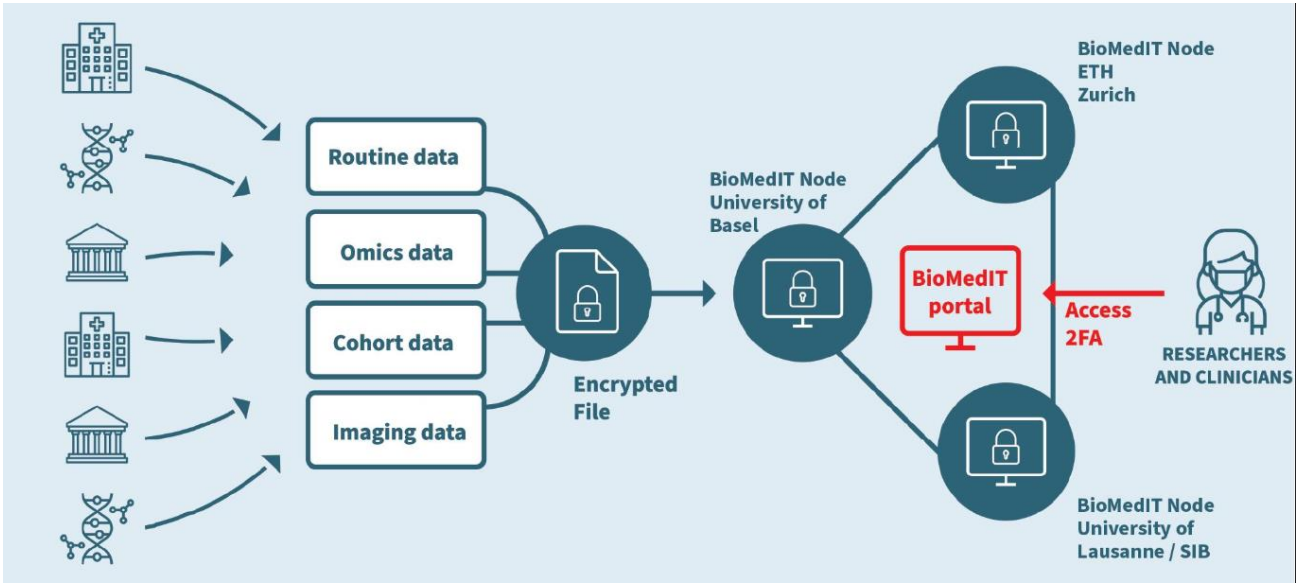
A secure IT environment for the responsible processing of health data:

– Data and (HP) computing services, cloud technology, remote access, collaborative analyses;

– Established network: **node Zurich (ETH Zurich), node Basel (Uni Basel) and node Lausanne (Uni Lausanne / SIB),** connected to Swiss data providers, end-to-end encrypted data transfers;

– Data protection and data security *by design*: **Organizational and tech. security measures** to guarantee confidentiality and integrity, as well as availability and resilience of the systems (Information Security Policy);

– Data remain on BioMedIT under the control of the consortium



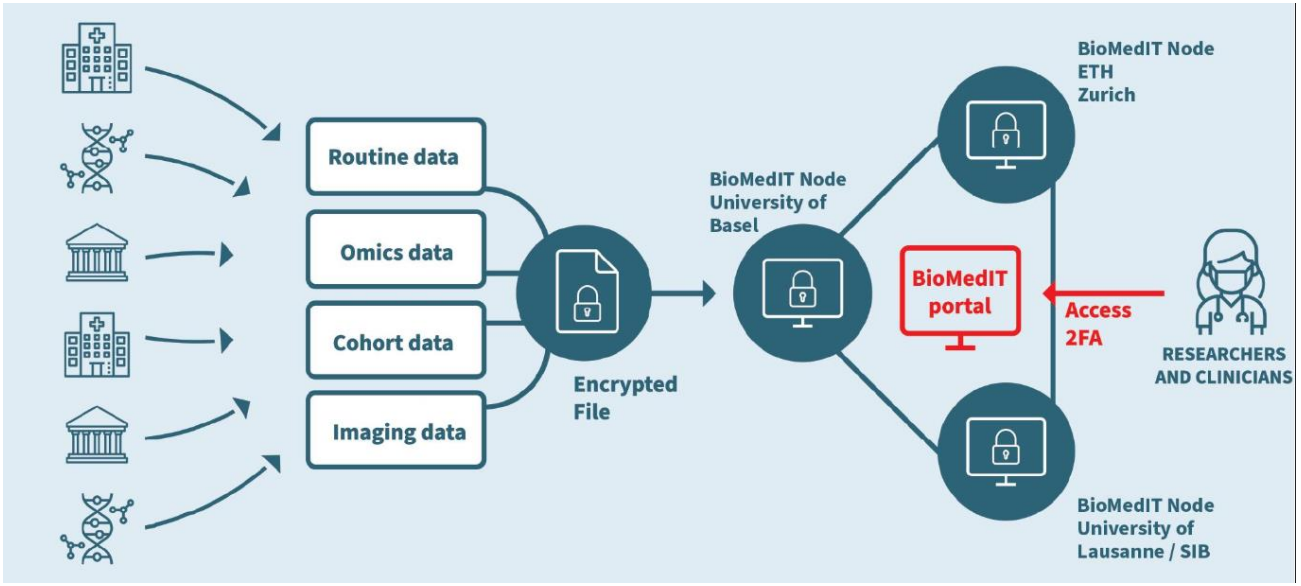
Data Transfer and Processing Agreement (DTPA)

Purpose: Regulates the relationship between Controllers and Processor(s) (e.g. BioMedIT node) by defining data access rules and minimum security requirements.

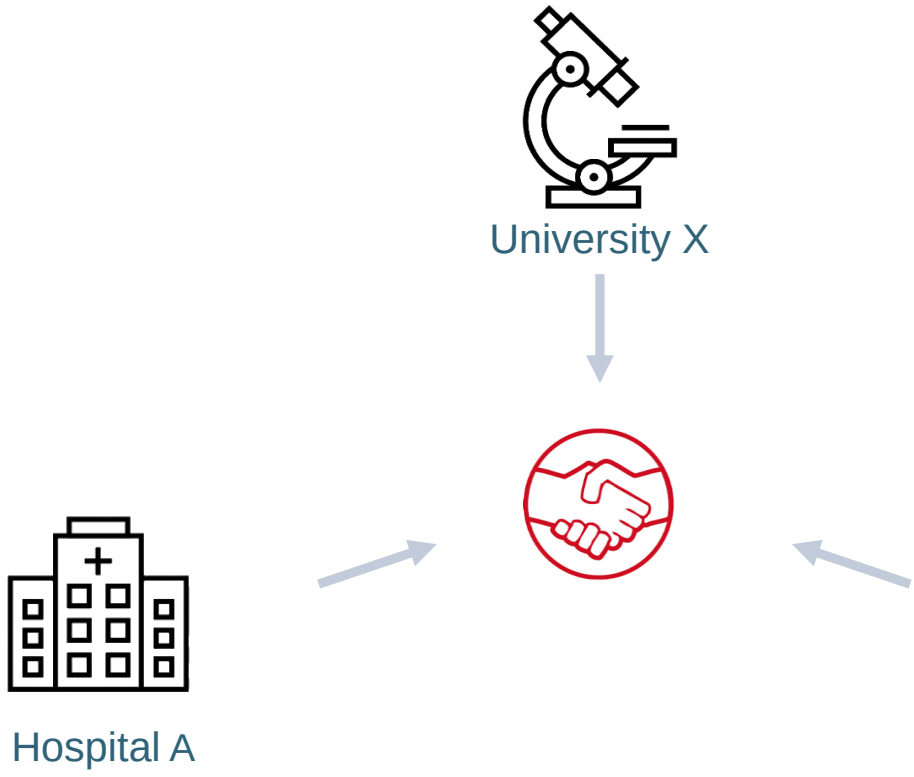
The processor acts as subcontractor according to the instructions of the controller.

Parties involved:

Parties to the DTUA and the institution(s) hosting (e.g. BioMedIT node Basel sciCORE)

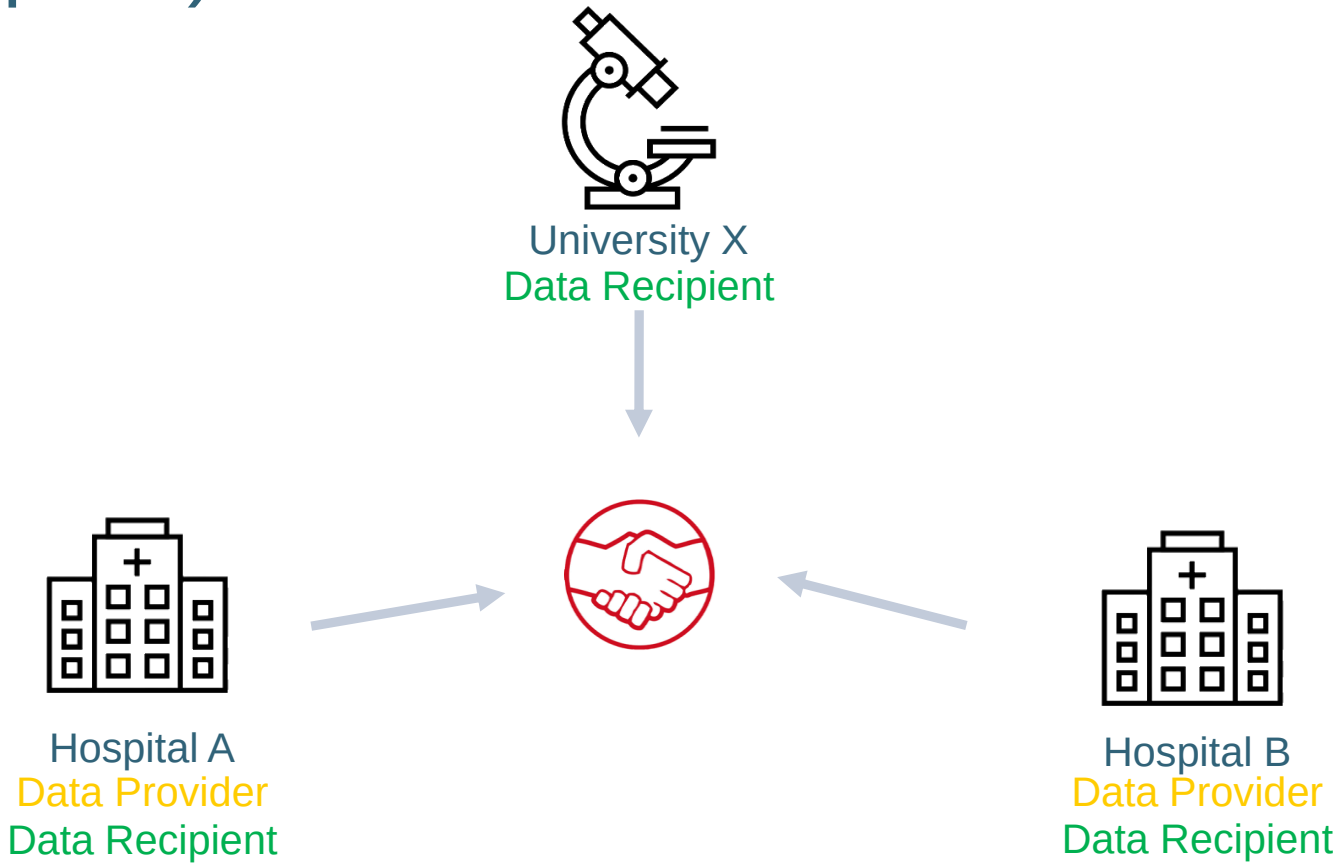


Defining the roles of research partners

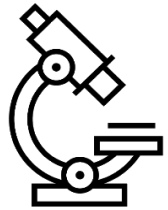


University X, Hospitals A and B wish
to conduct a collaborative project together,
which involves sensitive health-related data from
Hospitals A and B

Who discloses (data provider) and accesses (data recipient) data



Who discloses (data provider) and accesses (data recipient) data and controls data (data controller)



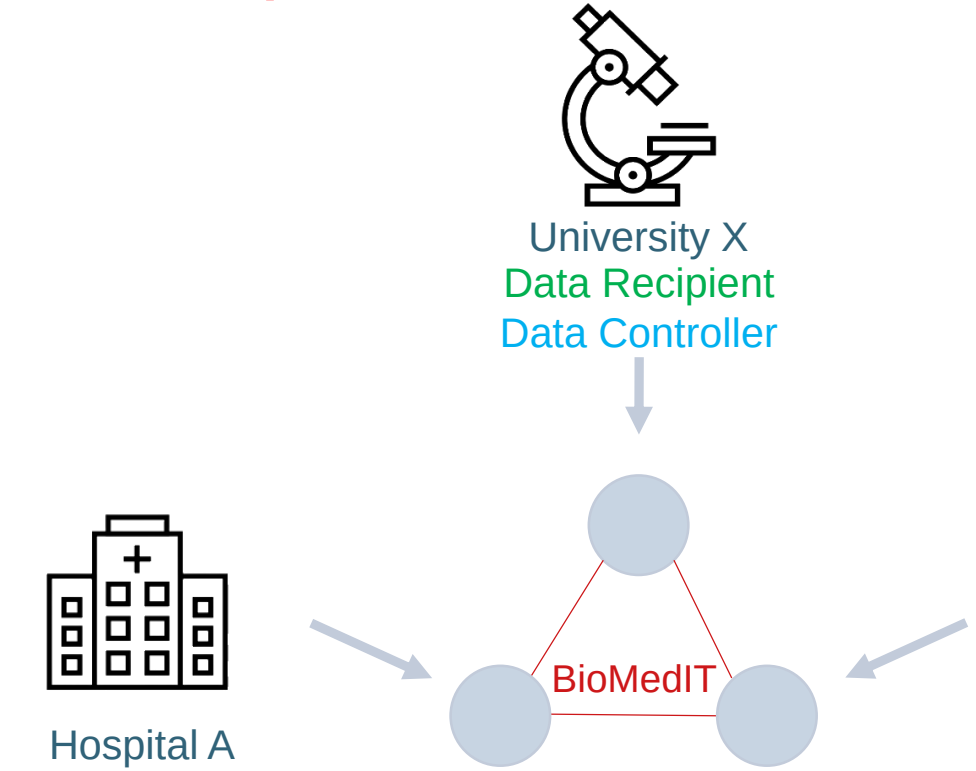
University X
Data Recipient
Data Controller

Hospital A
Data Provider
Data Recipient
Data Controller

Hospital B
Data Provider
Data Recipient
Data Controller

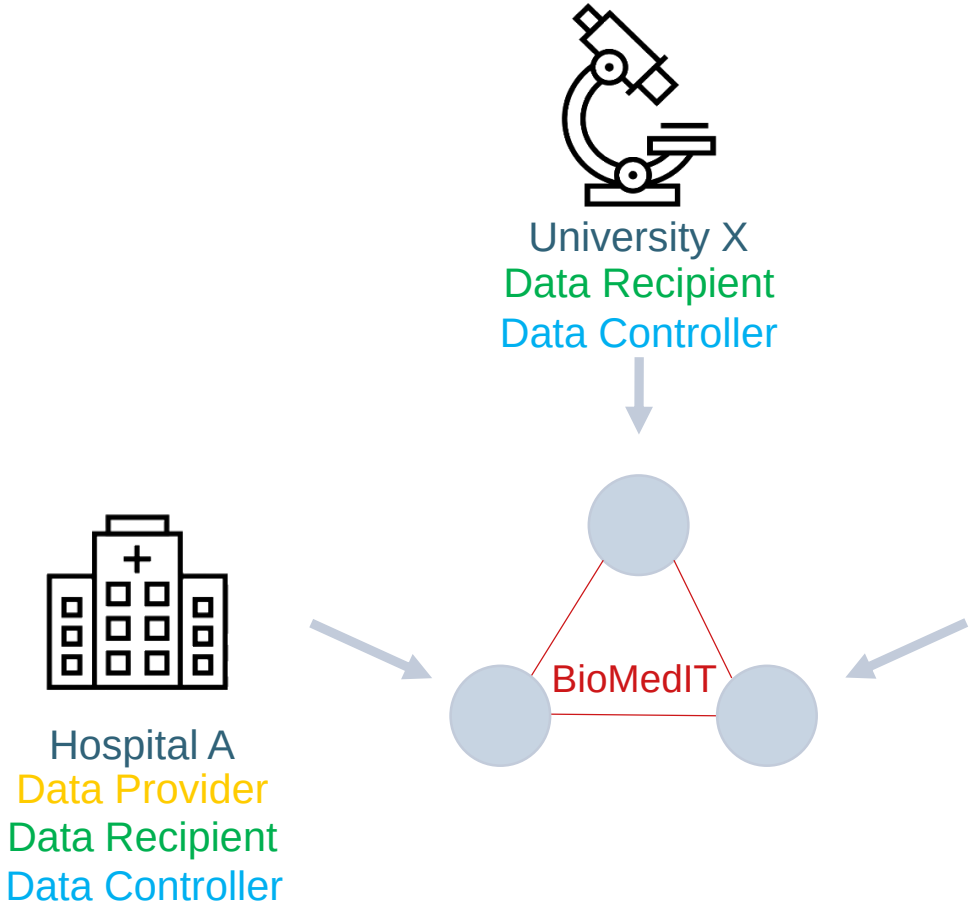
Provider and recipient define together the processing as joint controller.

Who discloses (data provider) and accesses (data recipient) data and controls data (data controller). Where are data processed?



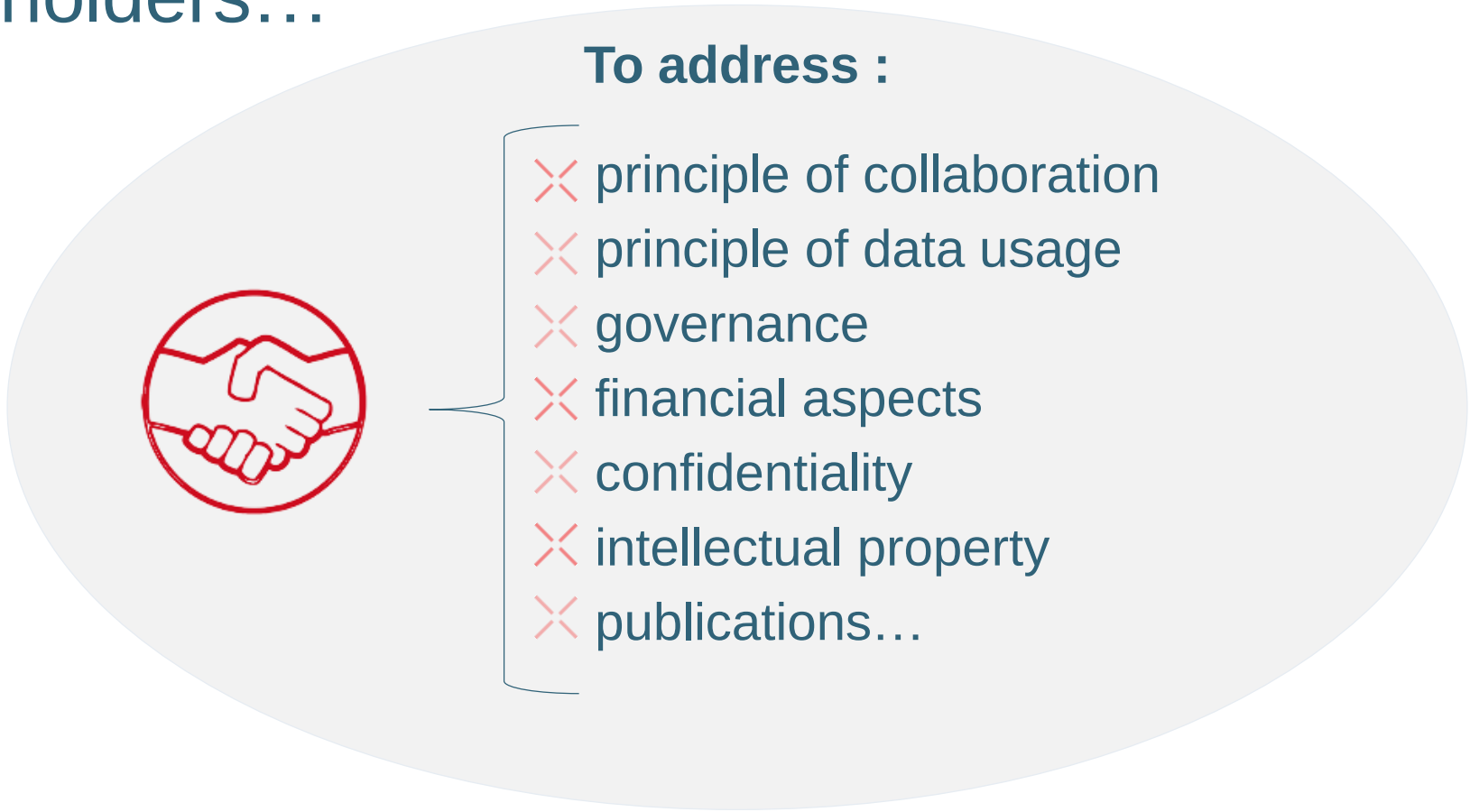
Provider and recipient define together the processing as joint controller. BioMedIT is used as external processor for hosting and transferring data

Who discloses (data provider) and accesses (data recipient) data and controls data (data controller). Where are data processed?

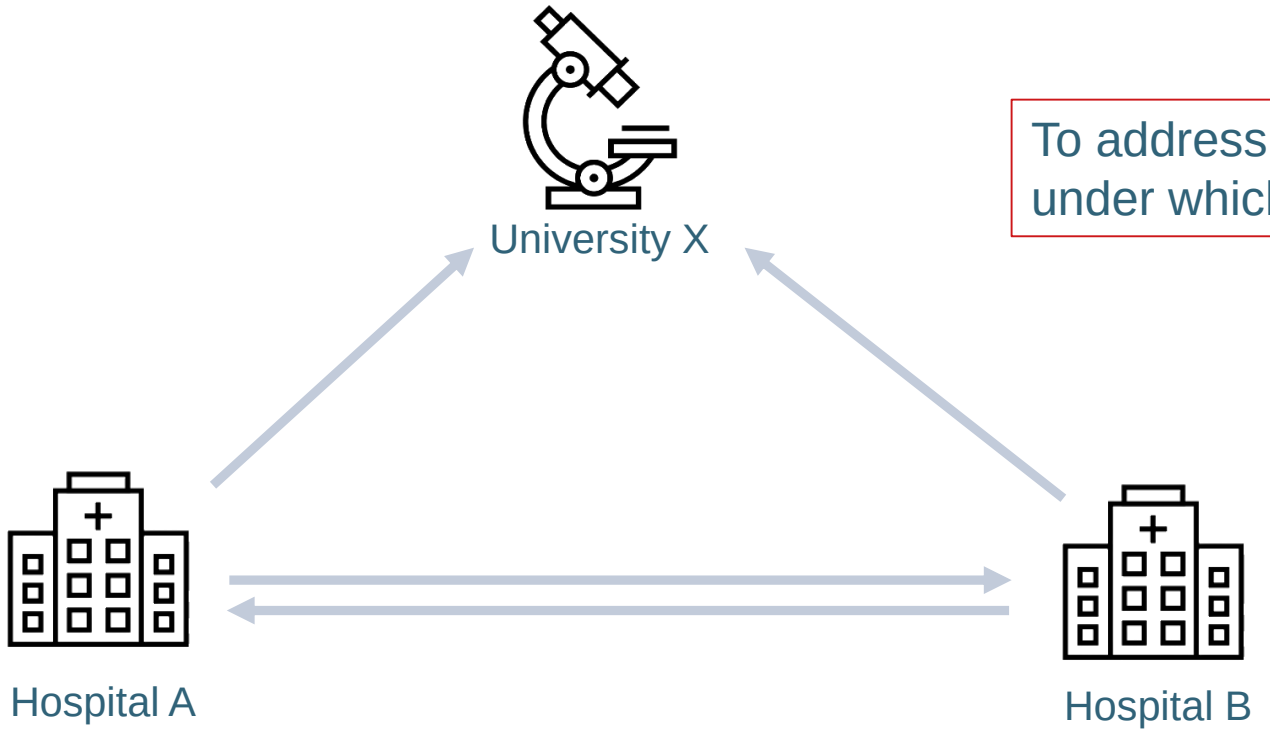


Set up of CA/ DTUA including DTPA

A general **Consortium Agreement** between the different stakeholders…

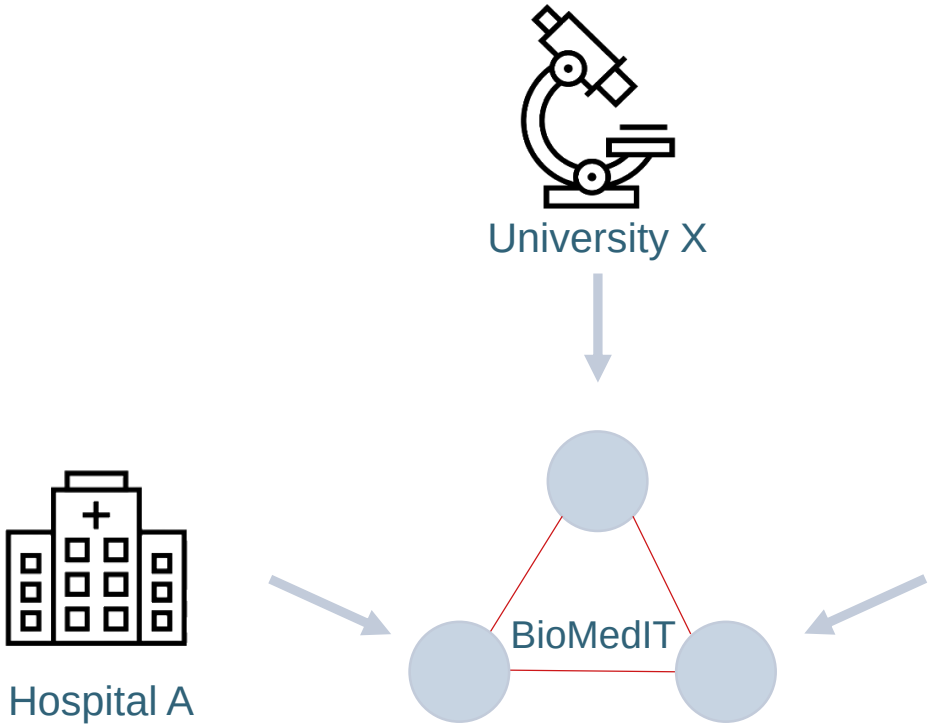


…with a **Data Transfer and Use Agreement** as an annex to the Consortium Agreement



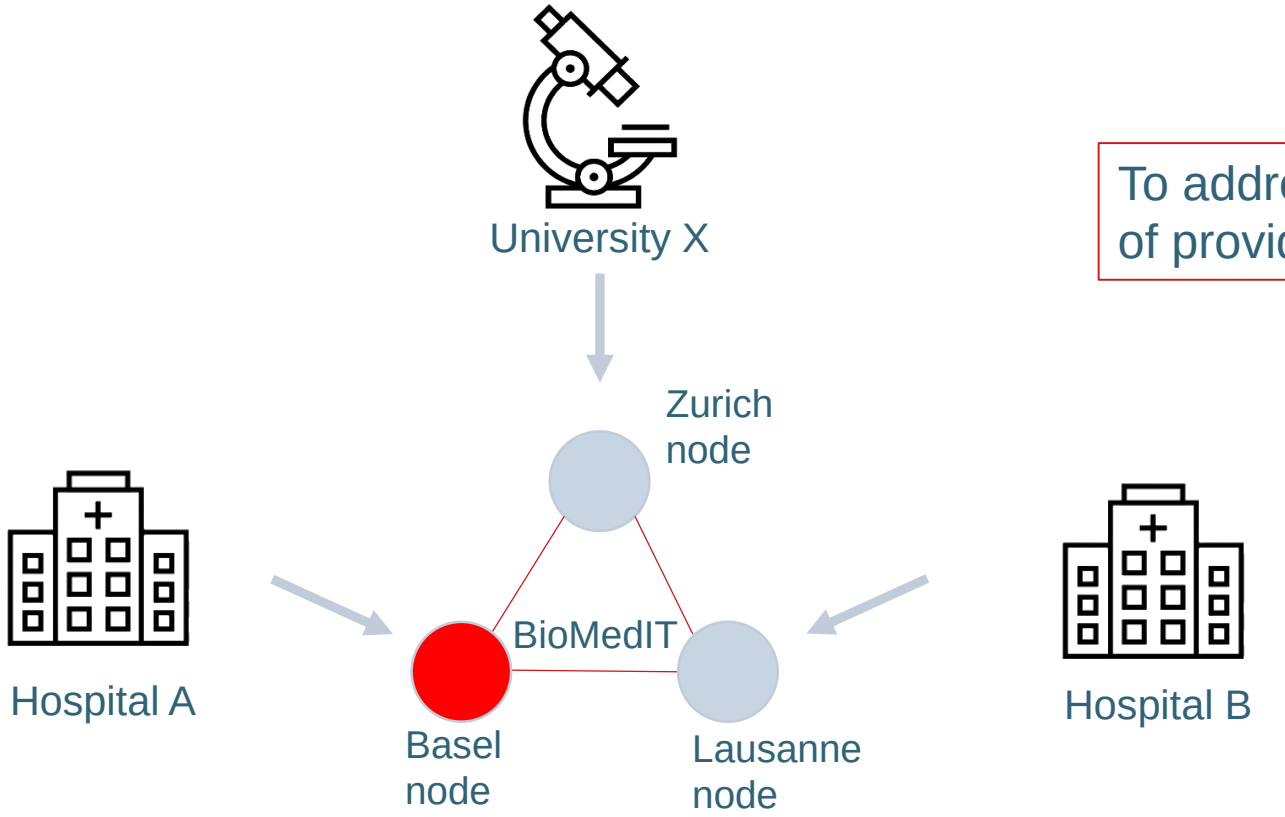
To address terms and conditions under which data are provided

…and if processing of data is provided as service by a third party (BioMedIT network), a Data Transfer and Processing Agreement (DTPA) is needed



To address terms and conditions of provided services

…and if processing of data is provided as service by a third party (BioMedIT network), a Data Transfer and Processing Agreement (DTPA) is needed



To address terms and conditions of provided services

Minimal Security Requirements in legal agreements

Technical and organizational measures (in responsibility of the recipient) to guarantee the confidentiality, integrity, availability and resilience of the systems regarding processing of data, such as

- Unauthorized persons are not able to access data processing system
- Unauthorized persons are not able to read and delete data in the system or during transport of data
- Ensure examination and verification when and by whom data was entered into the system
- Ensure adequate organizational measures to protect data

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 and necessary to conduct 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 guaranteeing the availability of: adequate confidentiality and data protection guidelines, regular data protection and privacy trainings, documentation 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.

Security measures

Minimal security requirements

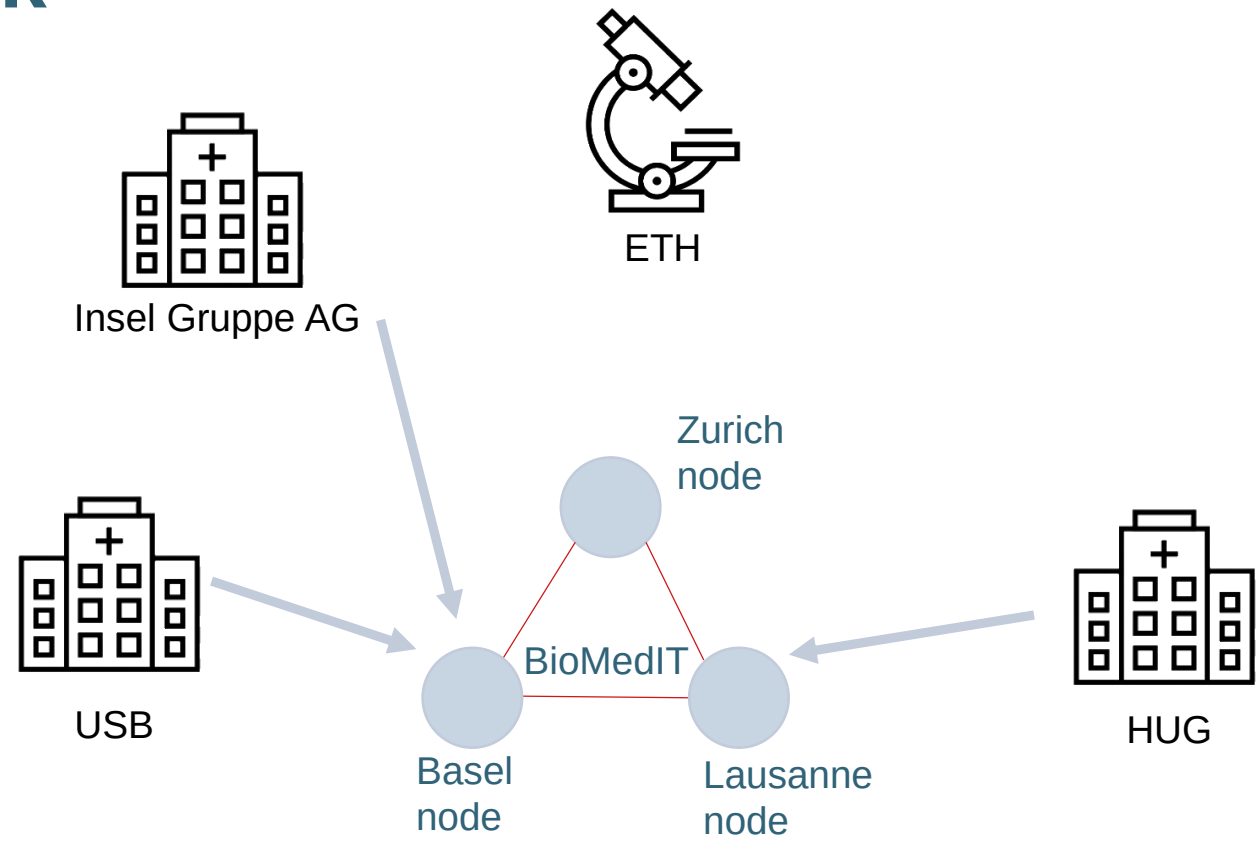
Technical and organisational measures (in responsibility of the recipient) to guarantee the confidentiality, integrity, availability and resilience of the systems with regard to processing of data, such as

- Unauthorized persons are not able to access data processing system
- Unauthorized persons are not able to read and delete data in the system or during transport of data
- Ensure examination and verification when and by whom data was entered into the system
- Ensure adequate organizational measures to protect data

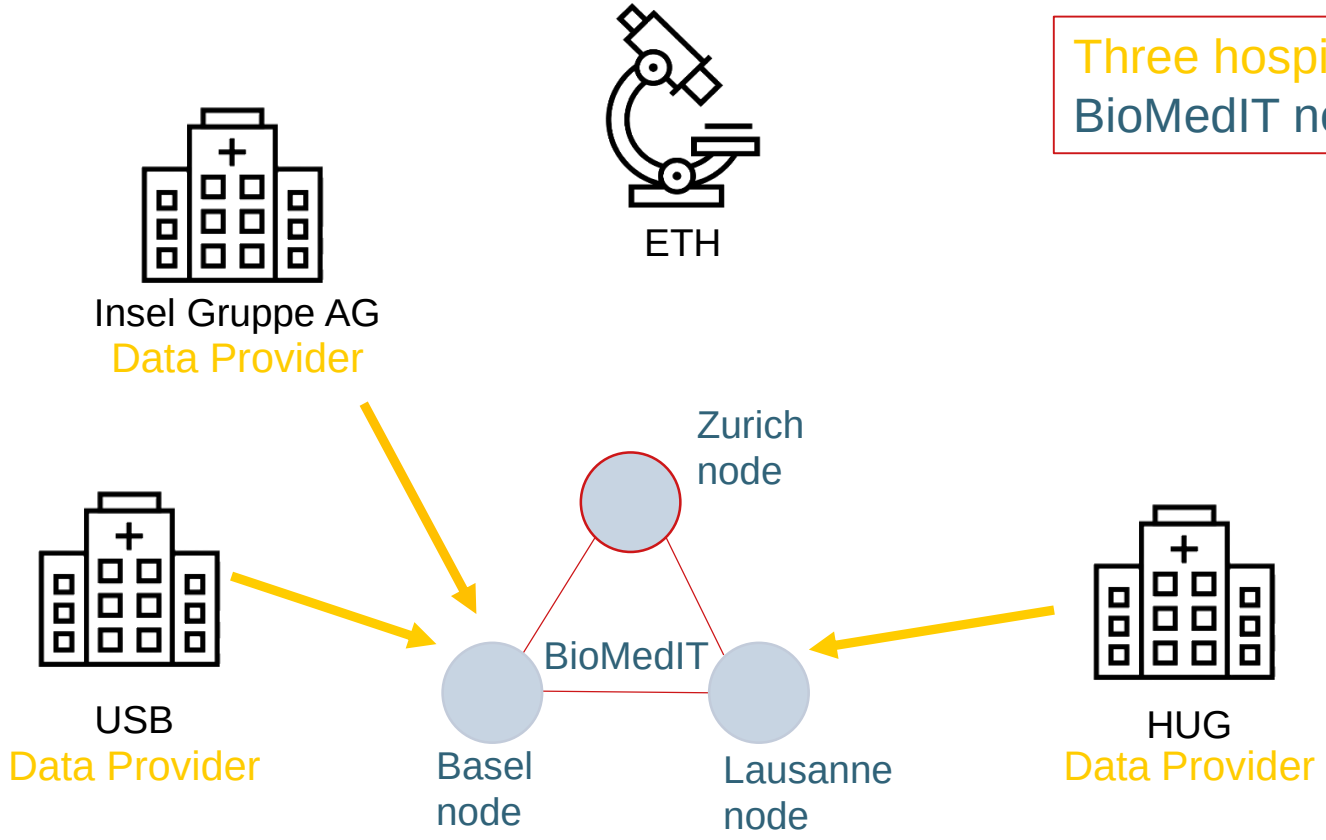
Information Security Policy for SPHN funded projects

- Provides management direction and support for “Information Security” in accordance with SPHN requirements, relevant laws and regulations.
- Controls the way the confidentiality, integrity, and availability of information is handled, preventing misuse

Use case of a multi-center research project with **4 parties** using data from **3 hospitals and BioMedIT network**

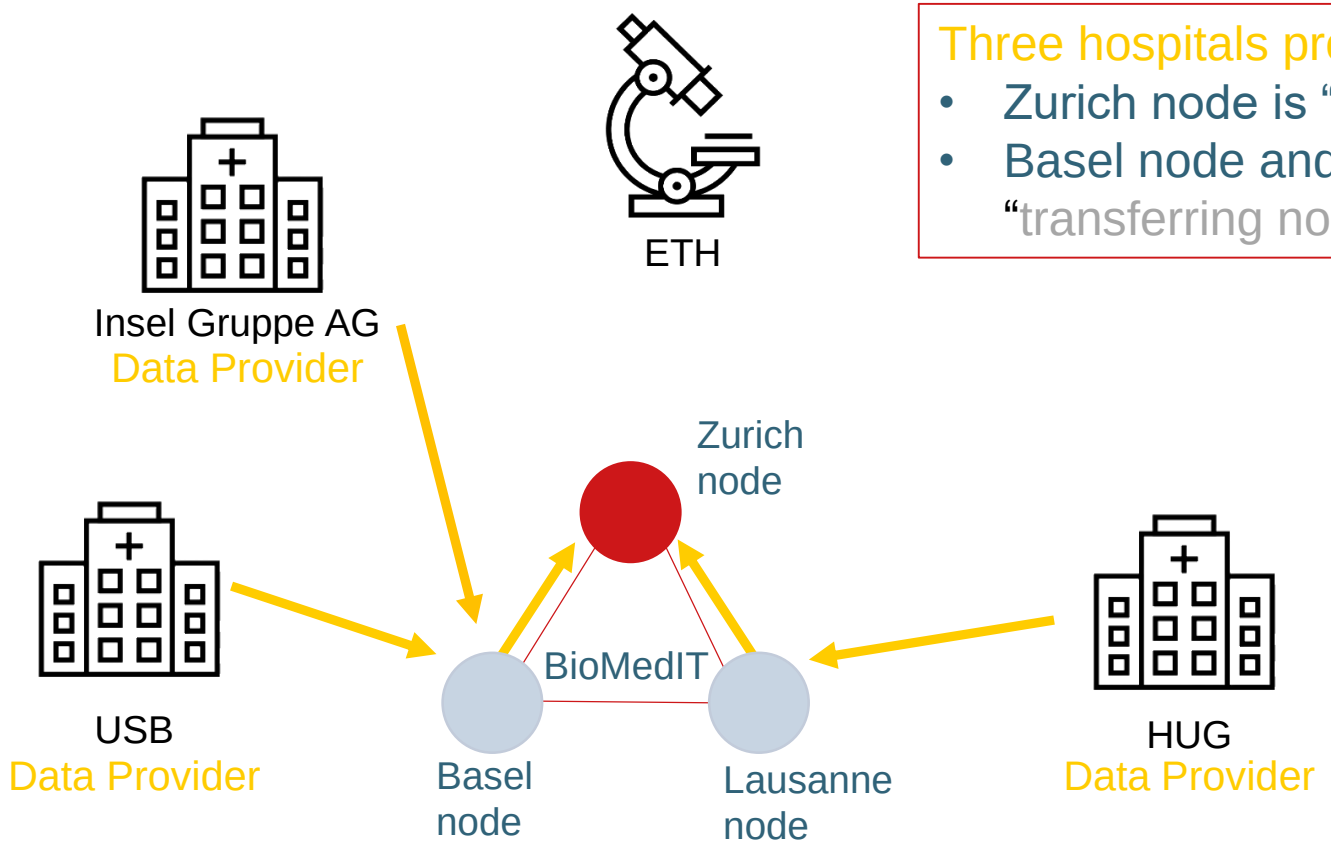


Use case: Defining the roles of parties (1)



Three hospitals provide data via BioMedIT network

Use case: Defining the roles of parties (2)

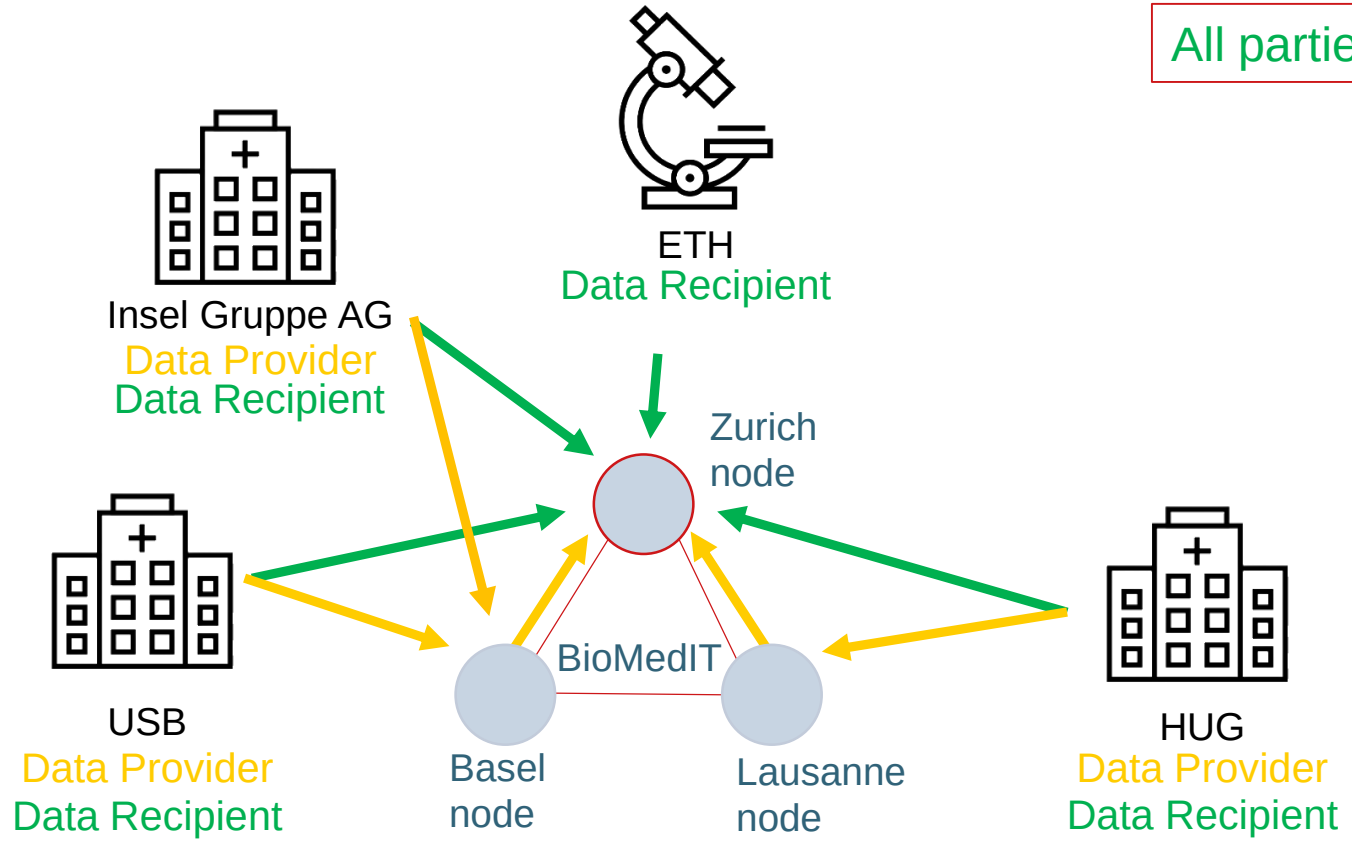


Three hospitals provide data via BioMedIT

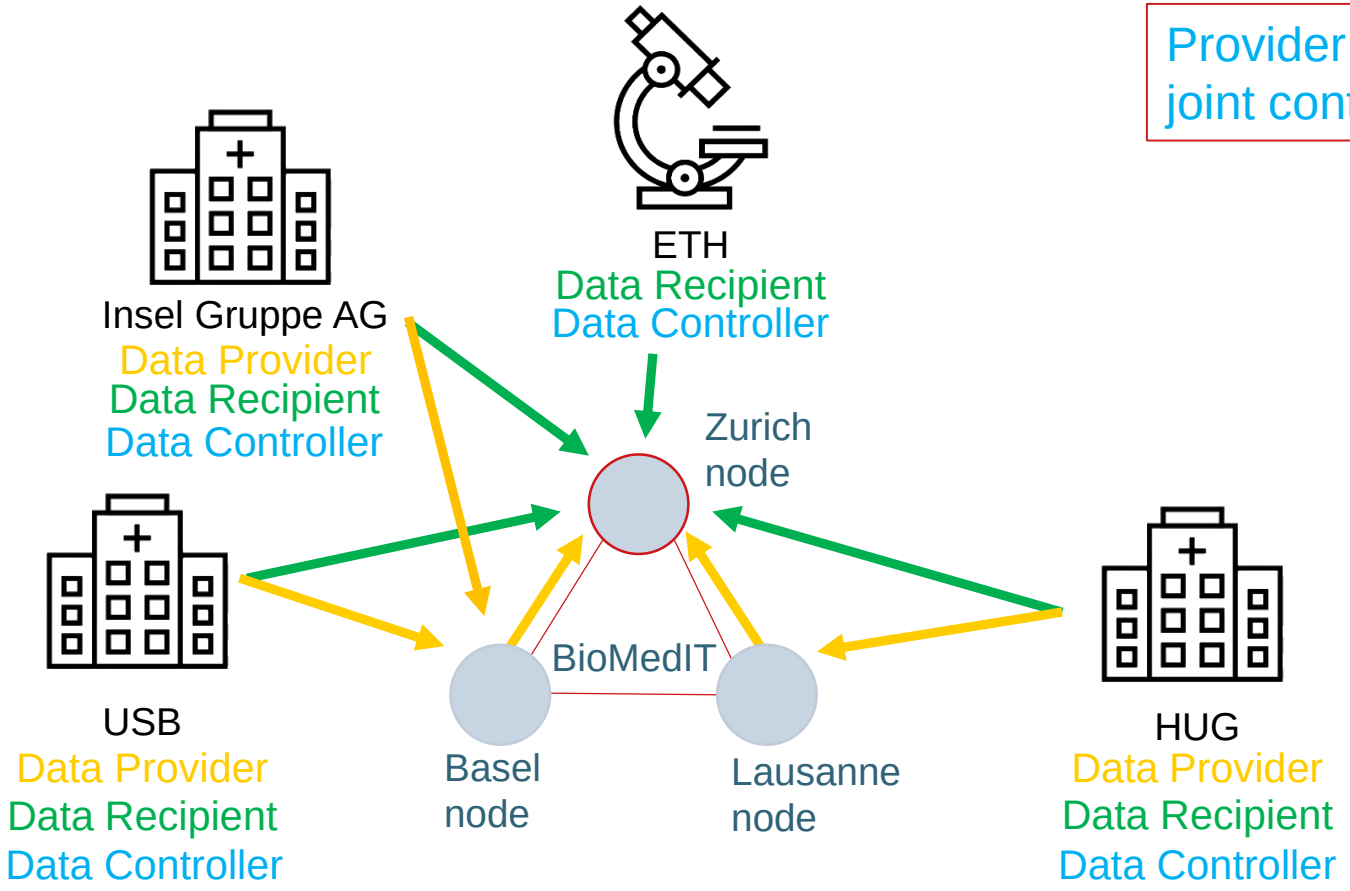
- Zurich node is "main node" for analysis
- Basel node and Lausanne node are "transferring node"

Use case: Defining the roles of parties (3)

All parties have access to data

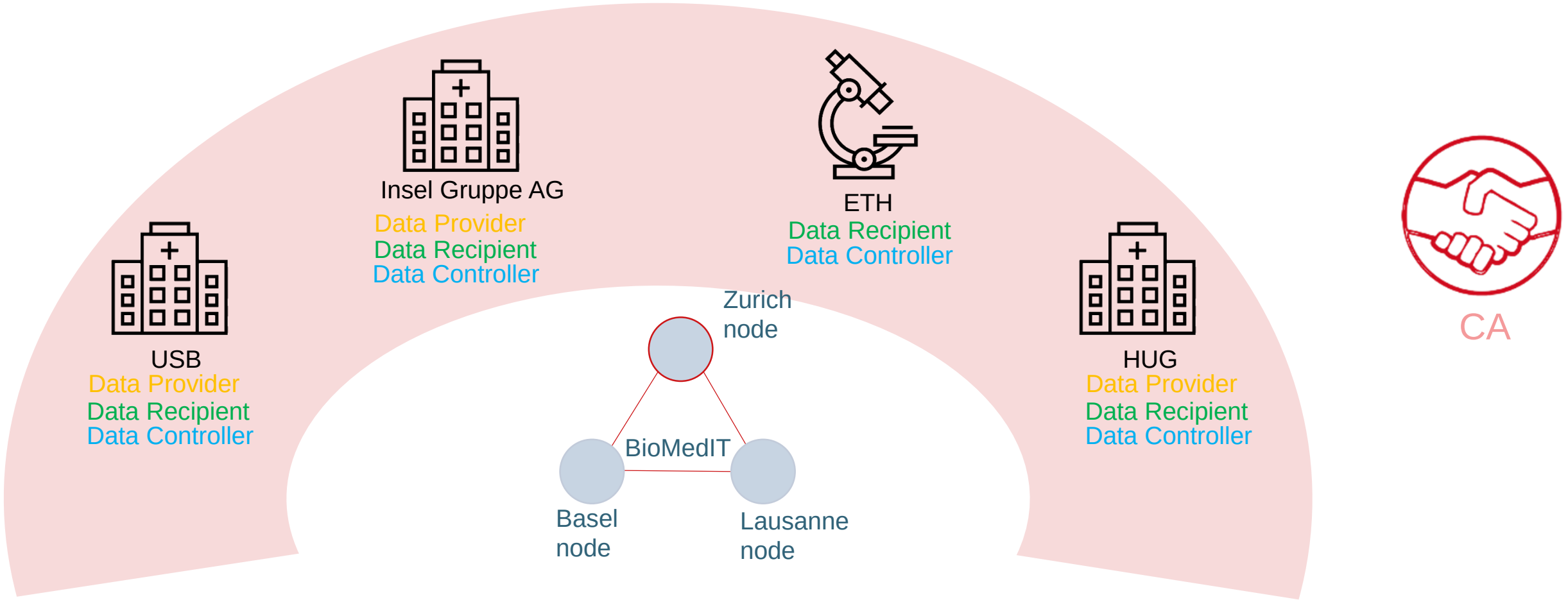


Use case: Defining the roles of parties (4)

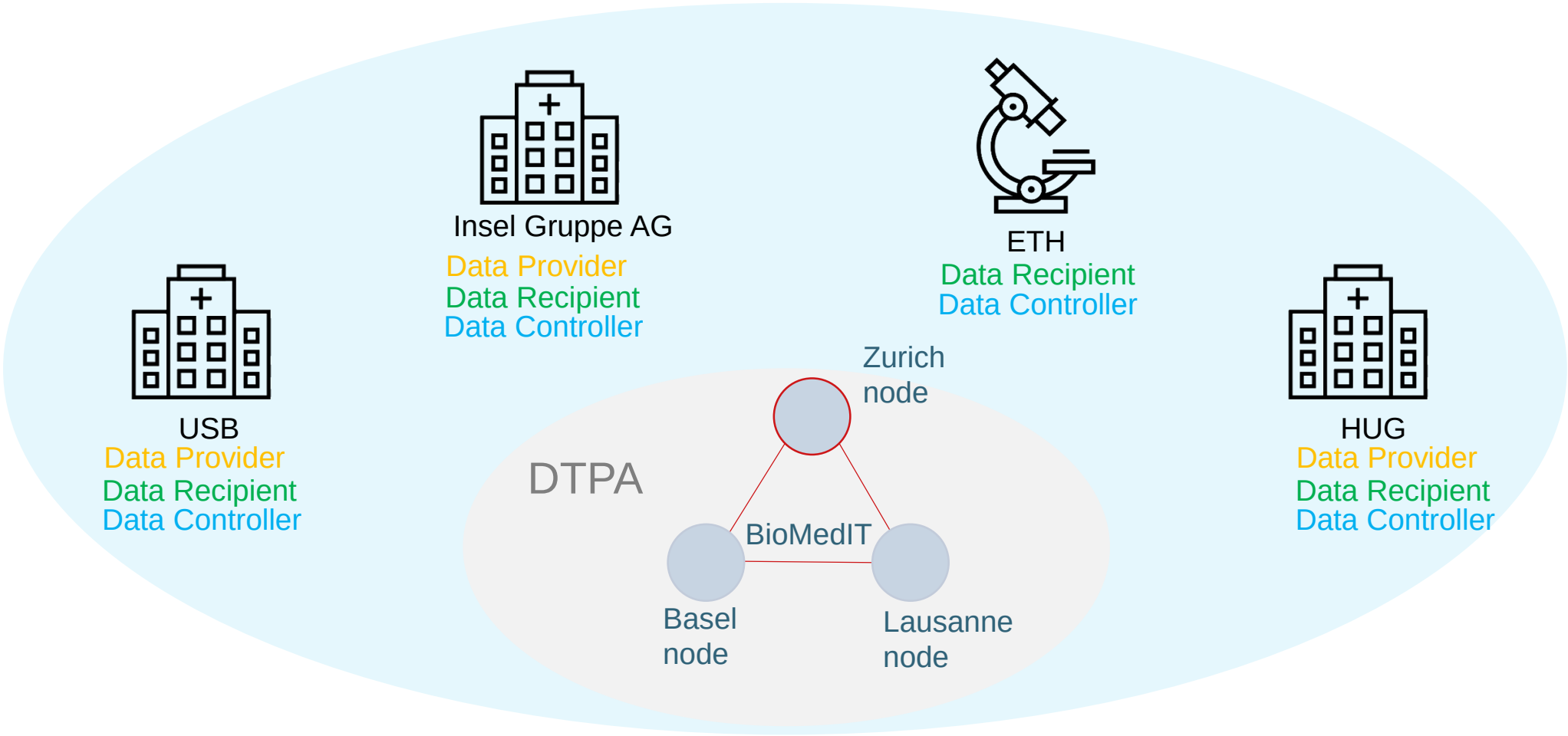


Provider and recipients are joint controller

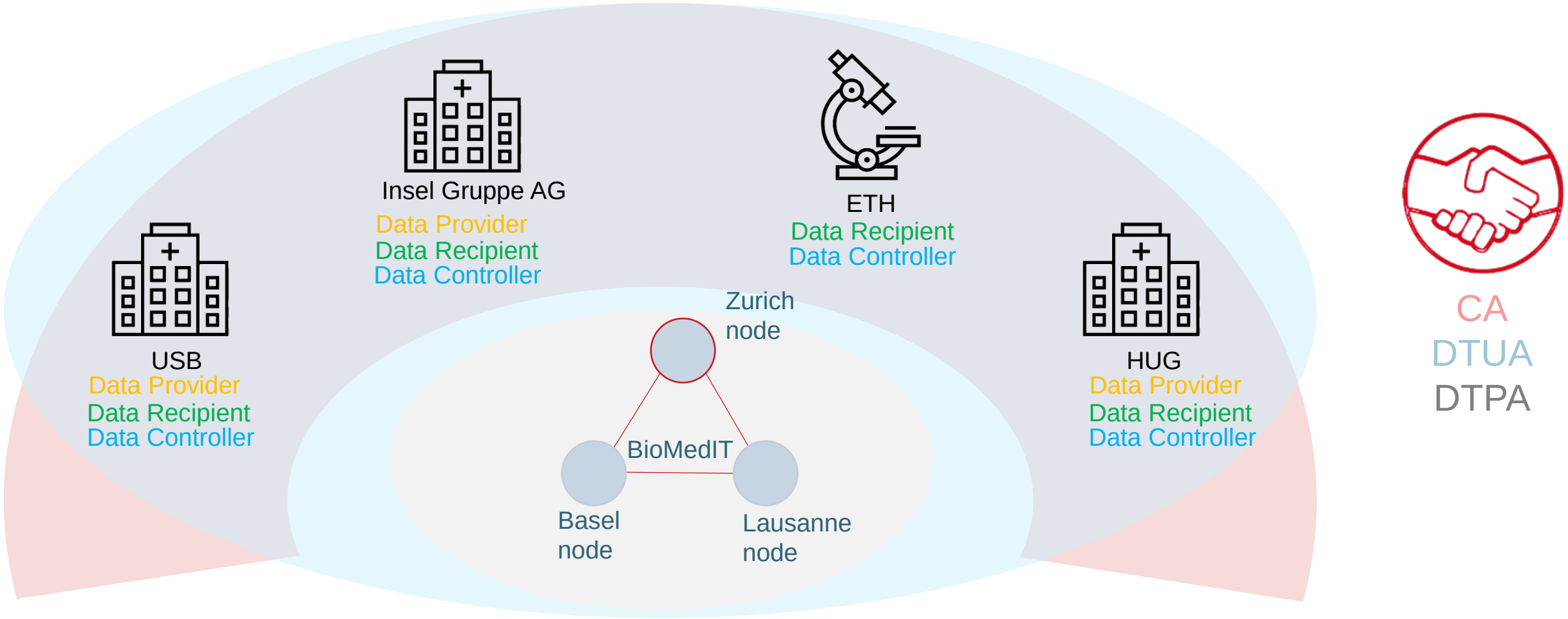
Use case: Set up of CA incl. DTUA +DTPA (1)



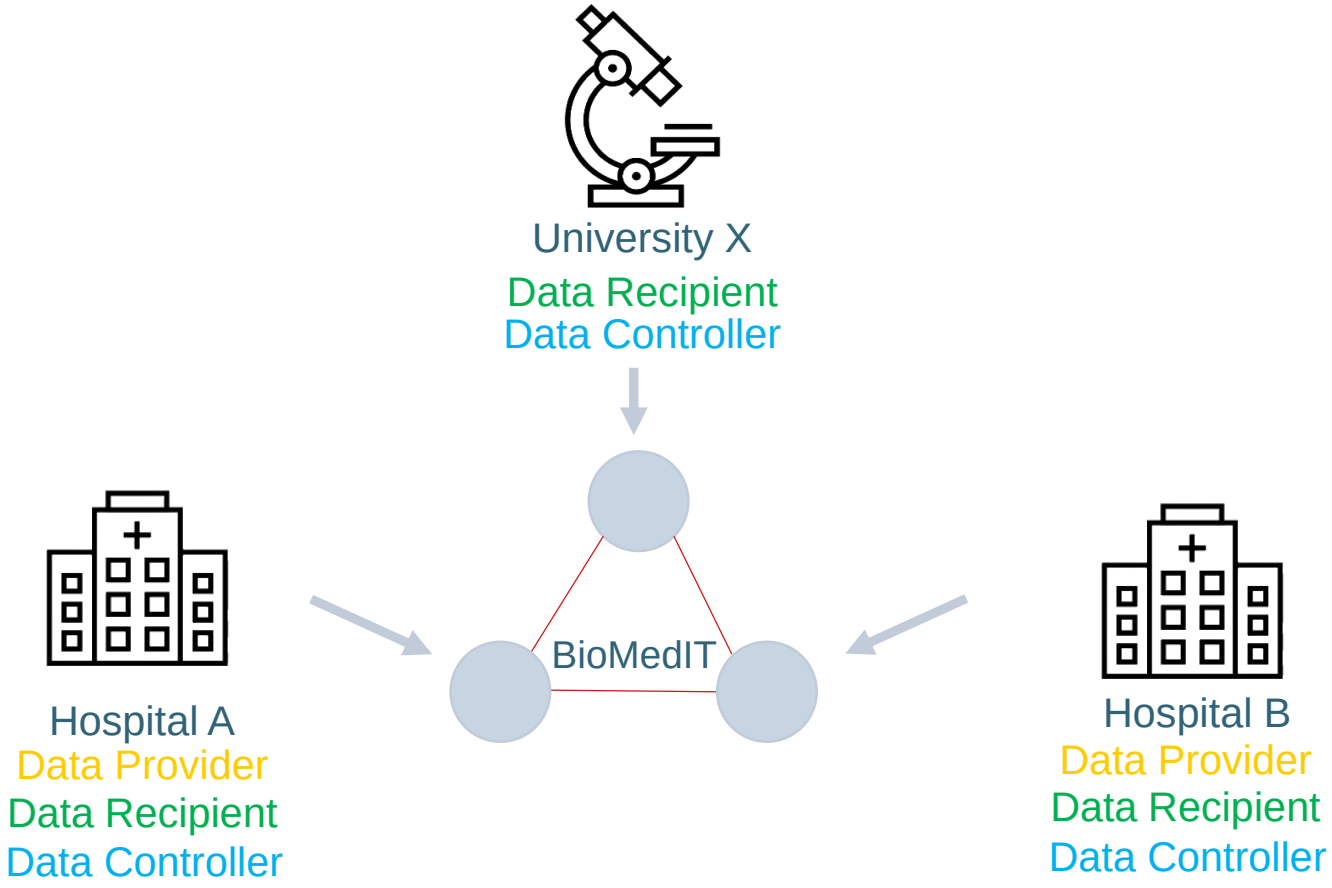
Use case: Set up of CA incl. DTUA +DTPA (2)



Use case: Set up of CA incl. DTUA +DTPA (3)

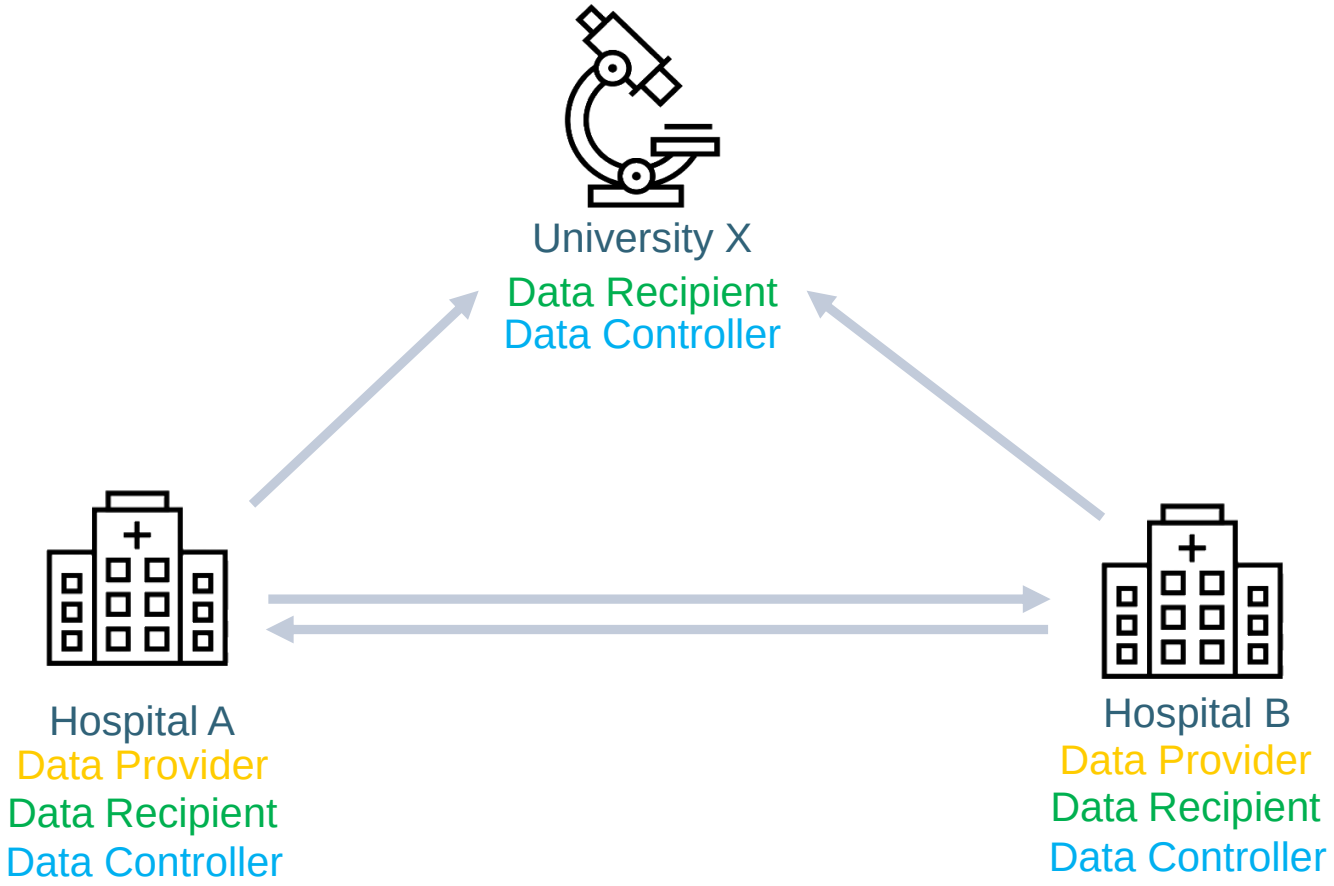


A full-fledged DTUA with external processor



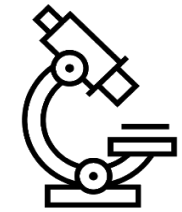
Consider already contractual undertakings

A full-fledged DTUA without external processor



Consider already contractual undertakings

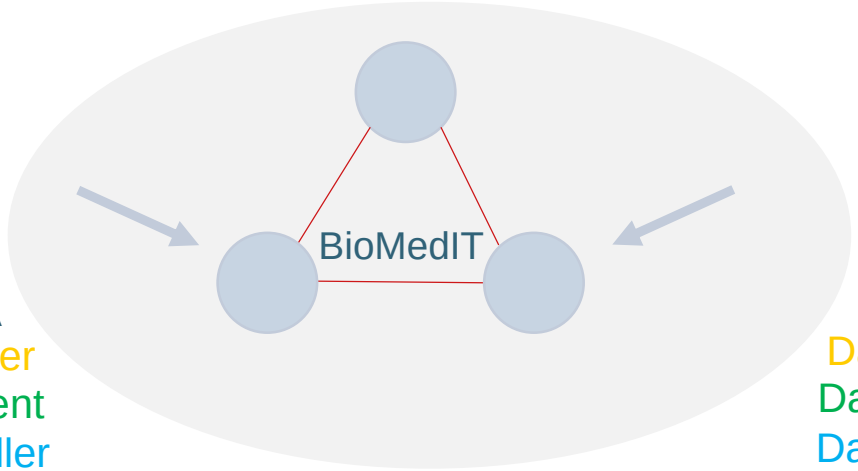
A Data Transfer and Processing Agreement only



University X
Data Recipient
Data Controller

If contractual agreements already in place

Hospital A
Data Provider
Data Recipient
Data Controller



Hospital B
Data Provider
Data Recipient
Data Controller

Available combinations of legal agreements

- CA
- CA incl. DTUA
- CA incl. DTUA+DTPA (multiple or single BioMedITnode)

- DTUA without external processor (BioMedIT node)
- DTUA incl. DTPA (multiple or single BioMedIT node)

- DTPA (multiple or single BioMedIT node)

Approval and signature process

Party (project partner):

Principal Investigators' home institutions and institutions required to provide data for the project

(e.g. University Hospital Basel (USB), Spitalstrasse 21 / Petersgraben 4, CH - 4031 Basel)

Signing persons:

- Duly authorized representative, entitled to sign the institutional data sharing in accordance with signatures rules of the institution (e.g. director of research department, member of the institution's executive board) or depending on internal processes additional persons sign (e.g. CEO).
- Responsible project leaders per institution/hospital, if applicable.
- For DTPA: Representatives of the BioMedIT nodes.

Signature (digital or paper-based):

Electronic unqualified signatures (e.g. using DocuSign) might be allowed if foreseen in the agreement, but, depending on the institutional process, a wet ink signature on paper might be required. Please contact your legal department to clarify the respective process, if needed.

Acknowledgements

The PHI Group:

Katrin Crameri, Sabine Österle, Shubham Kapoor, Julia Maurer, Michael Müller-Breckenridge, Kristin Gnodtke, Vasundra Touré, Jan Armida, Petar Horki, Martin Fox, Simone Guzzi, Patricia Fernandez Pinilla, Christian Ribeaud

The SIB LTTO: Marc Filliettaz, Frederic Erard

The SPHN NSB and NAB, Task Forces & WGs

The BioMedIT Board and workforces @ ETHZ, Unibas, Unil/SIB

The Hospital workforces @ USZ, USB, CHUV, Insel, HUG

The SPHN Management Office:

Thos Geiger, Liselotte Selter, Sarah Vermij, Cédric Petter

@SPHN_ch

dcc@sib.swiss I info@sphn.ch

www.sphn.ch I www.sib.swiss/phi
www.BioMedIT.ch