Revision of templates published by SPHN in January 2023

Background

The contractual architecture for a collaborative use and exchange of health-related data depends on the project specifications and responsibilities of participating parties, and is part of the legal and regulatory framework.

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

This DTUA Version 1.0 did not yet include a Processing Agreement covering the processing role of the BioMedIT network to be used in SPHN funded projects. This Processing Agreement part, as well as additional remaining aspects provided by some University Hospitals such as

- Minimal security requirements
- Information and Audits of Security Measures

were integrated in the agreement represented as the DTUA Version 2.0 including a Data Transfer and Processing Agreement (DTPA).

The DTUA Version 2.0 was officially released in November 2020 (after two DTUAs based on Version 2.0 have been approved by the legal departments of all University Hospitals, ETH and Universities) and published on the SPHN webpage. Moreover, templates for a Consortium Agreement including a DTUA/DTPA were developed.

Change requests have been expressed in order to ensure, in particular, appropriate confidentiality, integrity, availability and resilience of the systems with regard to processing of the Data. Therefore, we would like to address the changes in Version 3.1 of provided legal agreement templates.

Purpose

Revision of current published legal agreements templates (Consortium Agreement(CA), CA/DTUA/DTPA, DTUA/DTPA and DTPA) with Version 3.0 and release of updated legal agreement templates Version 3.1.

Change history in detail for Version 2.0, 3.0 and 3.1 (please note that this change history is provided exemplary for the CA/DTUA/DTPA multiple nodes):

Content	DTUA/DTPA 2.0	DTUA/DTPA 3.0	CA/DTUA/DTPA 3.1
In general		Colour code instructions added, providing a guidance text for completing the template; Change history added; Links updated	
Data provision I.6 'Effective date' wording changed	**EFFECTIVE DATE**: means the date when the first PARTY	**EFFECTIVE DATE**: means the date when this Agreement is signed by the	

	signs this Agreement.	duly authorized representatives of two PARTIES, and then for each additional PARTY, the date when the authorized representatives of such PARTY adhere and sign this Agreement.	
Data Processing III.2 Security			**Security**. The Recipient shall process the Data in a manner that ensures appropriate confidentiality, integrity, availability and resilience of the systems with regard to processing of the Data. The Recipient must in particular ensure appropriate protection against unauthorized or unlawful Data access or processing in any form (e.g., reading, copying, altering) and against accidental loss, destruction or damage, using appropriate technical or organizational measures. The effectiveness of such measures shall be regularly assessed, and corrective measures shall be immediately implemented in case of suspected data security breach. The Recipient shall have in place procedures so that access to the Data is only granted to identifiable persons who require it to conduct the specified research project. The Recipient shall adopt adequate organizational measures ensuring that any person authorized to access the Data: - is diligently and appropriately selected, instructed and supervised, in particular through

			the availability of adequate confidentiality and data protection guidelines, regular data protection and privacy trainings, documentation of all organizational measures; - respects and maintains the confidentiality and security of the Data; - processes the Data only on instructions from the Recipient's Project Leader; - does not combine the Data with other data unless explicitly authorized by the competent ethics commission for the specific research project and to the extent necessary to conduct the specific research project. The technical and organizational measures adopted by the Recipient must ensure that it is possible to examine and verify if, when and by whom Data was processed. The Recipient agrees to immediately report to the Provider (i) any actual or suspected data protection breach, including a breach against applicable data protection regulation, data protection section of this DTUA, (ii) any actual or suspected impairment or inadequacy of the Recipient in fulfilling data protection section of this DTUA, and (iii) any application to receive or any actual access to data by an authority, unless such reporting is not admissible under statutory provisions. 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 the Consortium Agreement or this DTUA; or (ii) sell, lease, sublicense, copy or provide the Data to any third party, except as expressly permitted in the Consortium Agreement or this DTUA. Except as provided above, the Recipient processes the Data in accordance with the "Ethical Framework for Responsible Data Processing in Personalized Health Research" and the "SPHN Information Security Policy", as both updated occasionally, accessible at: https://sphn.ch/document/ethical-framework/ https://sphn.ch/document/information-security-policy/
III.11 Download of data from the BioMedIT nodes			**Download of DATA from the BioMedIT Nodes.** Except with the prior written agreement of the Data Provider, the Recipient is not allowed to download or extract from the BioMedIT nodes Data related to identified or identifiable data subjects. For the sake of clarity, Data related to identified or identifiable data subjects includes "coded data" within the meaning of the Human Research Act and pseudonymized data.
Scope DTPA III.2			**Scope**. The Services consist of the standard services provided by the BioMedIT Nodes as described in the BioMedIT Base Package (accessible at: https://sphn.ch/document/biomedit-base-package) which include the following: a) hosting of the DATA on the BioMedIT Nodes;

			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, and as agreed on with the BioMedIT node. Computational and storage resources that exceed the limits set for the BioMedIT base package, will incur a service fee to the project. Services provided by the BioMedIT Nodes that fall out of the scope of this DTPA according to this Section III.2 (standard services provided by the BioMedIT Nodes) are regulated by separate service agreement between the BioMedIT nodes and the Party of the Consortium Agreement needing more capacity.
Security DTPA IV 3.1 Security requirements adapted; ANNEX IV with minimal security requirements is deleted			Security Requirements. Each PARTY shall comply with the security requirements set forth in Section III.3 of the DTUA. Security Requirements. The BioMedIT Nodes shall process the Data in a manner that ensures appropriate confidentiality, integrity, availability and resilience of the systems with regard to processing of the Data. The BioMedIT Nodes must in particular ensure appropriate protection against unauthorized or unlawful Data access or processing in any form (e.g., reading, copying, altering) and against accidental loss, destruction or damage, using appropriate technical or organizational measures. The scope of persons authorized to access the Data is determined according to the instructions given by the Recipient's Project Leader to the BioMedIT Nodes, provided that the BioMedIT Nodes personnel have the

			right to access the Data to the extent necessary for providing the Services. The BioMedIT Nodes shall adopt adequate organizational measures ensuring that the BioMedIT Nodes personnel: - respects and maintains the confidentiality and security of the Data; - processes the DATA only on instructions from the Principals; - is diligently and appropriately selected, instructed and supervised, in particular through the availability of adequate confidentiality and data protection guidelines, regular data protection and privacy trainings, documentation of all organizational measures. The BioMedIT Nodes must ensure that logging mechanisms exist which allow authorized personnel to inspect which Data was accessible by whom and when. The effectiveness of security technical and organizational adopted by the BioMedIT Nodes measures shall be regularly assessed, and corrective measures shall be immediately implemented in case of suspected data security breach. The BioMedIT Nodes process the Data in accordance with the “Ethical Framework for Responsible Data Processing in Personalized Health Research” and the “SPHN Information Security Policy”, as both updated occasionally, accessible at: https://sphn.ch/document/ethical-framework/ https://sphn.ch/document/information-security-policy

BioMedIT Nodes Intern Policies DTPA VII. 1. c)	**Acceptable Use Policy**. The PRINCIPALS undertake to comply with the Acceptable Use Policy specific to each REGIONAL NODE.	**Regional Node's Policies**. Provider undertakes to comply with the Acceptable Use Policy and other internal policies (e.g., service level agreement) specific to each Regional Node. Provider also undertakes, within the framework of its agreements with the Recipient, to require the Recipient to comply with such regulations.	
Liability DTPA VIII. 1.	Subject to Section VIII.2, each PARTY shall be liable to 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.	The parties agree to each be solely responsible for all acts or omissions in the performance of their respective duties hereunder, and shall be financially and legally responsible for all liabilities, costs, damages, expenses and attorney fees resulting from, or attributable	

		to any and all such acts or omissions.	
Terms DTPA IX.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.	**Term**. This DTPA shall become effective on the date when it is signed by the duly authorized representatives of one BIOMEDIT NODE, and then for each additional BIOMEDIT NODE, on the date when the duly authorized representatives of each additional BIOMEDIT NODE adhere and sign this DTPA. This DTPA shall remain in effect until expiration or termination of the DTUA, unless terminated earlier in accordance with this Section of IX of the DTPA.	
Terms DTPA IX 5 Further needs after termination of DTPA added			**Further Needs after the termination of the DTPA**. DATA hosting needs after the termination of the DTPA such as for long-term archiving or for making DATA available for other research projects, shall be regulated by separate agreement. Principals wishing to benefit from such further services shall notify the BIOMEDIT NODES at least three (3) months

			before the termination of this DTPA. In any case, such a notification does not affect this DTPA, including its termination clauses (Section IX). The BIOMEDIT NODES have no obligation to enter into a new agreement and shall in no event be held responsible for any interruption of the Services, in particular the DATA hosting activity.
General Provisions/Miscellaneous DTPA IX.3 and DTPA X.3 'Electronic form' wording adapted	**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.	**Counterparts and Electronic form**. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original and all of which shall together be deemed to constitute one and the same Agreement. Each Party acknowledges that an original signature or a copy thereof, including a "portable document format" or PDF copy, or a signature generated by industry standard electronic signature software (e.g. DocuSign),	

		which is transmitted by email shall constitute an original signature for purposes of this Agreement and shall have the same legal force and effect as the exchange of original signatures; while the term “in writing” shall include communications by email or other electronic forms.	