Terms of Use
LAST UPDATED ON JULY 01, 2022

General Terms and Conditions for the Use of Quentry

"Quentry" refers to the services available at quentry.com, www.quentry.com and all sub domains ("Services") provided subject to these General Terms and Conditions ("Terms"). "You" or "Your" refers to the individual, company or other legal entity for which you are accepting these Terms. Brainlab refers to Brainlab AG as the service provider of Quentry.

1. Acceptance of Terms

1.1 These Terms shall govern the contractual relationship between You and Brainlab and Your use of Quentry and applications/elements available through Quentry. If You use a free trial of applications/elements through Quentry, these Terms shall also govern Your free trial. Further terms and conditions shall apply upon purchase of a paid premium subscription package, feature, or application.

1.2 Either by checking the box indicating Your acceptance of these Terms, which is displayed as part of the registration process, or logging into Quentry, You agree to be legally bound by the Terms for using Quentry. If You do not agree with these Terms, You should not accept the Terms and should not register to use Quentry.

1.3 If You are accepting these Terms on behalf of a company or other legal entity, You represent that You have the authority to bind such entity to these Terms.

2. Subject Matter; User License

2.1 Quentry provides a web based software for medical professionals that (i) supports users to build a global clinical network, (ii) provides an online community to work in virtual groups and (iii) provides users with tools for secure online image (e.g. DICOM, jpg, word, ppt, excel, zip) storage, review, transfer and sharing (collectively "Intended Use"). QUENTRY IS NOT INTENDED FOR PRIMARY DIAGNOSIS, UNLESS EXPLICITLY STATED OTHERWISE, AND IS NOT INTENDED FOR DETAILED TREATMENT PLANNING OR TREATMENT OF PATIENTS. "User Data" shall mean any

information or data submitted, disclosed or shared by You within the online community. "Patient Data" shall mean any data belonging to patients to be shared with and/or transferred to other users expressly selected and authorized by You.
2.2 Unless authorized by You, Brainlab shall not take part in any communication between You and other users. If You enter into any agreement or communication with another user by using Quentry, in no event shall Brainlab become a contracting party to such agreement nor be responsible or liable, directly or indirectly, for any duty, damage or loss caused or alleged to be caused by or in connection with such agreement or communication.
2.3 Subject to the Terms and for the duration of Your Account (as defined below), Brainlab grants to You a personal, limited, non-transferable, non-exclusive right to access and use Quentry in accordance with these Terms, the user manual and the respective service description of the selected subscription and/or available under quentry.com/learn and/or terms and conditions of sale, as applicable, however, restricted to the Intended Use ("User License").
2.4 You acknowledge and agree that it is technically impossible to achieve 100% availability of Quentry. In particular, Brainlab shall not be responsible or liable, directly or indirectly, for any unavailability of Quentry caused by circumstances beyond Brainlab's reasonable control, including without limitation, acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving Brainlab employees), or internet service provider failures or delays. In the event of planned downtimes, Brainlab will give at least 8 hours prior notice, if feasible.

3. Registration

3.1 You must register prior to using Quentry by entering all required user information displayed as part of the registration process. You shall not use pseudonyms or pen names. Your Brainlab ID will not be visible for any person outside of the Quentry Services.
3.2 You warrant and represent that any information provided by You for registration ("Registration Data") is accurate and complete. In the event of any changes in the Registration Data, You shall correct such data without undue delay. Due to the fact that Brainlab is unable to verify whether any user registered with Quentry is in fact the person he/she represents to be, Brainlab assumes no liability or responsibility for any inaccurate or incomplete user information or noncompliance with these Terms among users.
3.3 You warrant and represent that (i) You are (a) a physician or medical physicist with valid license to practice according to applicable law or a team member of such physician or medical physicist, or (b) an IT administrator associated with a physician or medical physicist with valid license to practice according to applicable law, or (c) a healthcare-related professional that has obtained Brainlab's prior written approval to use the Services, and (ii) the only purpose of Your registration is to use Quentry in the course of Your professional activity and within its Intended Use, and (iii) You are of legal age at the time of registration, however at least 18 years, having full legal capacity. Brainlab reserves the right to contact You in order to verify Your representation and Registration Data. For verification, You are obliged to provide adequate proof upon request. Brainlab may disable access to Your user account until receipt of proof.
3.4 You shall keep Your password secret at all times and avoid disclosing Your password to any third party including Brainlab at all times. Brainlab will not ask for your password at any time. You agree to accept responsibility for all activities that occur under your password.

3.5 Your registration for Quentry in the course of the online click-through process shall be deemed to be Your agreement to abide by the Terms including any materials available on Quentry incorporated by reference herein. By activating Your user account, Brainlab accepts Your request to use Quentry.
3.6 Unless otherwise expressly agreed in writing, You are entitled to register with Quentry only once. You may only establish one (1) user account and may not share Your account with any other user or any other individual.
3.7 Unless otherwise expressly agreed in writing, You shall not register for and use or access Quentry if You are a direct competitor of Brainlab or offering similar services. In addition, You shall not access Quentry for purposes of monitoring its availability, performance or functionality, or for any other benchmarking or competitive purposes. In case of violation, Brainlab may terminate Your Account with immediate effect.

4. User Obligation; Restrictions on Use

4.1 While using Quentry, You shall be responsible for Your compliance with the Terms, and be solely responsible for Your actions performed under Quentry and the contents of all User Data and Patient Data posted, submitted or otherwise disclosed by You, including its accuracy, quality, integrity and legality.
4.2 You shall not submit or otherwise disclose Patient Data that contain personal identifiable information relating to other individuals, unless You have obtained prior voluntarily informed written consent from the individual concerned or otherwise permitted by applicable law. When submitting or otherwise disclosing Patient Data through Quentry, You warrant and represent that You are authorized to transfer and disclose such data, either by having obtained informed consent from the person concerned or by being duly authorized in accordance with applicable law, and that such transfer and disclosure is not prohibited by any applicable law. Whenever possible, You shall only submit or disclose anonymized or otherwise de-identified data that do not contain personal identifiable information relating to other individuals. You shall not use Patient Data for any other purposes than those specified by the disclosing user. Upon request of the disclosing user or any person entitled, You shall immediately cease using and delete such Patient Data.
4.3 Physicians, medical physicists and other healthcare professionals are bound by medical confidentiality. Therefore, when using Quentry, healthcare professionals are responsible for (a) anonymization of patient data according to applicable laws and regulations or (b) obtaining patients prior written release from medical confidentiality according to applicable laws and regulations. This written release from medical confidentiality has to refer to the processing of Protected Health Information (PHI) at Quentry.com, a web-based Service owned and operated by Brainlab AG, Germany. It also has to comprise that in case of catastrophic event requiring a data recovery and for necessary maintenance of the Service, PHI may be transferred to Brainlab AG's subsidiary Brainlab Ltd., Israel.
4.4 You shall not use Quentry for any purpose that is unlawful or prohibited by these Terms. You acknowledge and agree that Quentry is released for use in specific countries listed on the FAQ. You agree and acknowledge that access to Quentry from countries not expressly specified is strictly prohibited. You shall comply with all applicable local, state, national and foreign laws, treaties, regulations and third-party rights, including, without limitation, those related to data privacy, international communications, the transmission of technical or personal information, and government regulations.
4.5 You agree that when using Quentry, You will not
4.5.1 modify, decompile, reverse engineer, disassemble, attempt to discover the

source code or algorithms of, or create derivative works based on, any of the Services or any part thereof, or access Quentry in order to build a competitive product or service or to copy any ideas, features, functions or graphics of Quentry;
4.5.2 disable or circumvent any access control or related device, process or procedure established with respect to Quentry or any part thereof. Such prohibited conduct includes, without limitation, any efforts to gain unauthorized access to any Services, other user accounts, computer systems or networks connected to any of the Services, through hacking, password mining or any other means, log into an account with a password not assigned to You, access identifiable information not intended for You, test the security measures on Quentry and/or attempt to identify system vulnerabilities, attempt to disable Quentry, or interfere with the access, use of, or any activities conducted on Quentry by any other user;
4.5.3 transfer, resell, sublicense, rent, lease, lend, assign, copy or otherwise make Quentry available in whole or in part to any third party;
4.5.4 advertise to, or solicit, any user to buy or sell any products or services and to use the information obtained from Quentry in order to contact, solicit, advertise or sell any products or services to any user;
4.5.5 collect information about other users of Quentry for any purpose other than Your use as expressly permitted by these Terms;
4.5.6 distribute or publicly disclose the contents of Quentry or any other user, and/or any information related to Quentry, including but not limited to technical data, product descriptions, and any other information which is readily and reasonably identifiable as confidential based on its nature and/or the circumstances of its disclosure;
4.5.7 use Quentry to send or store infringing, obscene, threatening, libelous, or otherwise unlawful or tortuous material, including material harmful to children or in violation of third party privacy rights, send spam, contests, pyramid schemes, chain letters, junk emails or otherwise duplicative or unsolicited messages, send or store material containing software viruses, worms, trojan horses, malicious code, or other harmful computer code, files, scripts, agents or programs;
4.5.8 defame, abuse, harass, stalk, threaten or otherwise violate the legal rights (such as rights of privacy and publicity) of other users of Quentry or any third party;
4.5.9 use without authorization any contents protected by law, such as by copyright, trademark, patent, utility patent, or design patent laws, or advertise, promote, offer or distribute any goods or services protected by law.
4.6 You shall refrain from using Quentry beyond its Intended Use, notify Brainlab immediately of any unauthorized use of any password or account or any other known or suspected breach of security, report to Brainlab immediately and use reasonable efforts to stop immediately any copying or distribution of content that is known or suspected by You using Your account, and not impersonate another user or provide false identity information to gain access to or use Quentry.
4.7 You shall be responsible for obtaining and maintaining of technical equipment, resources and other requirements needed to access and use Quentry, including but not limited to computer hardware, software, communication devices and internet access ("Equipment"). Any costs arising out of or in connection with the Equipment shall be borne by You. Details on technical requirements for using Quentry are set forth in the Technical Facts Sheet which is available under "Help" after logging-in.
4.8 Without limiting the foregoing, Brainlab may disable, restrict access to or the availability of Quentry if it determines any of the restrictions on use have been violated. Brainlab may also delete any content, information or other material that Brainlab deems to be illegal, offensive or otherwise in violation with the Terms.

5. Subscriptions; Fees; Free Trial; Payment

5.1 Quentry offers two types of subscription accounts: a User Account for individuals and a Business Account for organizations, herein collectively referred to as “Account”. Individual User Accounts are provided at no cost via online signup form at quentry.com, and may be upgraded by You with premium subscription packages, subscription-based features, and/or application licenses (“Paid Subscription(s)”) which are subject to additional fees. Business Accounts are provided when purchasing Paid Subscription(s). Details on Paid Subscriptions are provided on quentry.com. Please contact Your Brainlab sales representative in order to purchase Paid Subscription(s).

5.2 Brainlab may make one or more Services or applications available to You on a trial basis free of charge until the earlier of Your or Brainlab's termination at any time, the end of the trial expiration period, or the start date of any subscription period or Paid Subscription(s) ordered by You. Additional trial terms and conditions may appear in the course of the registration for such trial and shall be incorporated into these Terms. Unless terminated by You or Brainlab during the trial period or otherwise stated, Your free trial will turn into and continue as a Individual User Account after expiration of Your free trial.

5.3 Additional Integration Services: Use of downloadable Quentry DICOM integration tools may require purchase of additional licenses and/or services. Brainlab shall provide such installation and/or configuration services upon Your request at Your cost.

6. Responsibility for User Data and Patient Data

6.1 You shall be solely responsible for any User Data and Patient Data posted, submitted or otherwise disclosed by You and verification of the identity of any other user You share such data with and/or transfer such data to. You are also required to follow the rules and regulations of Your professional law. Brainlab will not monitor, examine, supervise or otherwise control any exchange of data, nor content of User Data and Patient Data.

6.2 User Data and Patient data will be stored in an encrypted database. You acknowledge and agree that Brainlab and/or third-party access may not be completely excluded for Your Brainlab ID information (Brainlab ID, email address and password hash). You are solely responsible to ensure that Your User Data does not contain any protected patient information or any other sensitive or confidential information. You acknowledge and agree that other users may search for and see user profile and/or group profile details including contact information, unless You selected to hide such profile information.

6.3 Brainlab does not make any warranties or representations regarding any User Data or Patient Data and/or information provided or made available by any user on Quentry or on any external website linked to it. Brainlab does not warrant or represent that any such data/or information is true or accurate, or that it fulfills or serves any particular purpose.

6.4 You shall report to Brainlab any activities of any other user of Quentry which violate applicable laws and/or any of these Terms.

6.5 Brainlab and/or its affiliates may offer remote support services in connection with the Services. You acknowledge and agree that, when using such remote support services, Brainlab and/or its affiliates may see Patient Data that contain personal identifiable information. You warrant and represent that You are authorized to disclose such data to Brainlab and/or its affiliates, either by having obtained informed consent from the person concerned or by being duly authorized in accordance with applicable law, and that such transfer and disclosure is not

prohibited by any applicable law. Whenever possible, You shall only disclose to Brainlab and/or its affiliates anonymized or otherwise de-identified data that do not contain personal identifiable information relating to other individuals. Physicians, medical physicists and other healthcare professionals are bound by medical confidentiality. Therefore, when using Brainlab remote support services, healthcare professionals are responsible for (a) anonymization of patient data according to applicable laws and regulations or (b) obtaining patients prior written release from medical confidentiality according to applicable laws and regulations.
6.6 Any such consent - besides to being in compliance with all applicable statutory requirements - has to include clear notice on the relevant personal data being potentially accessible for Brainlab AG, Olof-Palme-Straße 9, 81829 Munich, Germany, +49 89 99 15680, legal@quentry.com and other Brainlab entities (Brainlab Ltd. (Israel), Brainlab Inc. (USA)) and the storage on server instances of Amazon Web Services Inc., Ireland in an encrypted form. Brainlab shall have the right to request from You sufficient proof for obtaining proper consents. The above principles shall also apply to the releases from medical confidentiality, where required.
6.7 With the upload of a DICOM image you have the option to pseudonymize the image. After uploading the image You do not have the option to pseudonymize it any more. If you choose to pseudonymize the DICOM image, it is not anonymized in the meaning of data protection law, but pseudonymized by de-identification. If personal data is pixeled in the DICOM image, such data is not removed and the image is not de-identified. Information which you enter or uploaded files other than the above mentioned DICOM images are not de-identified.

7. Ownership; Third Party Licenses; Feedback

7.1 You acknowledge and agree that Brainlab and/or its licensors own all legal right, title and interest in and to the Service, and any software provided to you as a part of and/or in connection with Quentry ("Software"), including any and all intellectual property rights that exist therein, whether registered or not, and wherever in the world they may exist. You further agree that the Service and Software contain proprietary and confidential information that is protected by applicable intellectual property and other laws. You agree that neither You nor any third party shall obtain any express or implied rights in or to any part of Quentry.
7.2 For the avoidance of doubt, Brainlab does not claim ownership of User Data and Patient Data You submit or make available through Quentry.
7.3 In the event You elect, in connection with any of the Services, to communicate to Brainlab suggestions for improvements relating to Quentry ("Feedback"), Brainlab shall own all right, title and interest in and to the Feedback. Brainlab shall be entitled to use Feedback in its sole discretion and without restriction. You herby assign all right, title and interest in and to the Feedback to Brainlab and agree to provide Brainlab assistance as may be required to document, perfect, and maintain the rights to the Feedback.

8. Term and Termination

8.1 You may terminate Your User Account at any time without cause by providing written notice. Brainlab may terminate Your User Account without cause by giving thirty (30) days written notice to You.
8.2 Brainlab may terminate Your Account or parts of Services with immediate effect upon notice if You materially breach any of these Terms. In addition, Brainlab shall be entitled to delete User Data posted or submitted by You, issue a warning, and/or block Your access to Quentry until such material breach is cured.
8.3 Brainlab may also terminate Your Account or parts of Services with immediate effect upon notice (a) if any of the Services is not in conformity with applicable laws

and legal conformity cannot be ensured within a reasonable time, or the establishment of such conformity would be unduly burdensome or otherwise unlawful for Brainlab, or (b) in order to comply with applicable law or requests of governmental entities, or (c) if Brainlab's relationship with a third party who provides services or any other technology necessary to provide Quentry to You expires, terminates or requires Brainlab to change the way of use of such services or other technology as part of Quentry, or (d) Brainlab is no longer able to provide Services due to circumstances beyond Brainlab's reasonable control, or (e) if Brainlab has, in its sole discretion, decided to suspend or no longer offer Quentry by providing at least three (3) months prior notice.

8.4 Your Individual User Account and all rights thereto are personal and non-transferable and shall terminate in case of death with immediate effect, unless specified otherwise in Your purchase contract.

8.5 Upon termination of Your Account, Brainlab shall be relieved of any obligations to grant access to Quentry and to provide any Services. Notwithstanding the foregoing, any stored Patient Data that has been once uploaded by You to Your Account will be deleted.

9. Modifications

9.1 You acknowledge and agree that Brainlab may restrict, alter or reduce Services, or modify these Terms or any policy, agreement or other terms referenced in the Terms at any time by providing to You a revised version of the Terms or the respective document ("Revised Terms") in accordance with section 9.2 below. Modifications to the Quentry Privacy Policy shall be in compliance with the provisions set forth therein.

9.2 Brainlab will give You at least six (6) weeks' notice of any modification of the Terms by sending You an email. Revised Terms shall be deemed to have been approved by You, unless You indicate disapproval before the proposed date of entry into force of Revised Terms ("Effective Date"). Brainlab shall expressly draw Your attention to this consequent approval. Brainlab may also implement a mechanism for Your acceptance of Revised Terms, such as a click-through confirmation, a check-the-box confirmation or an acceptance button.

9.3 You acknowledge and agree that Your Individual User Account and Your continued use of Quentry is subject to Your acceptance of Revised Terms. If You disapprove or do not accept Revised Terms before the Effective Date, Your membership will terminate effective the end of the day prior to the Effective Date.

10. No Medical Advice

Brainlab is not a healthcare institution or medical facility and neither Brainlab nor Quentry provide any medical advice. You are solely responsible for all medical decisions, including the interpretation of any Patient Data, and any diagnosis, treatment or treatment plan, made by You as the result of the use of Quentry. You acknowledge that image capture, image processing and image display also depend on Your specific computer hardware environment and corresponding system settings which are beyond Brainlab's reasonable control. Brainlab does not warrant that the image representation through Quentry will be free from any hardware-based display errors such as image distortions, color deviations or poor contrast and brightness values. IT IS THE SOLE RESPONSIBILITY OF YOU AND ANY OTHER USER, PHYSICIAN OR MEDICAL PHYSICIST INVOLVED TO ANTICIPATE THE POSSIBILITY OF SUCH DISPLAY ERRORS IN INTERPRETING IMAGES VISUALIZED THROUGH QUENTRY.

11. Indemnification

11.1 You shall indemnify and hold harmless Brainlab from all actions, including claims, demands, suits, or proceedings made or brought against Brainlab by other

users or third parties resulting from an infringement of their rights by User Data or Patient Data disclosed by You, or regarding the use of Quentry by You. You assume all reasonable attorneys' fees, costs, and expenses incurred due to an infringement of third party rights. All other rights, including damage claims by Brainlab shall remain unaffected. You may give prove that Brainlab incurred lesser charges than claims made.

11.2 In the event any User Data or Patient Data disclosed by You infringes any rights of any third party, You shall, at Your own expense, either obtain the right to use such data or render such data free of any infringement. In the event You infringe third party rights when using Quentry, You shall discontinue such use that violates these Terms or applicable law.

12. Limitation of Liability

12.1. Brainlab shall be liable only for damages (i) to the extent they have been caused by Brainlab's negligent or willful breach of an essential obligation under these terms; liability for negligence in this respect shall be limited to forseeable damages; or (ii) to the extent they have been caused by gross negligence or intentional misconduct on Brainlab's part. Essential obligations are those that enable the realization of the contractual relationship in the first place and on observance for which the parties may regularly trust. The foregoing shall apply for any and all claims, including but not limited to tort claims.

12.2. The limitation of Brainlab's liability as set forth in 12.1. shall not apply to damages caused by Brainlab's gross negligence or wilful misconduct, bodily injuries, compromised health or death or to any claims under the German product liability act.

12.3. You shall indemnify and hold harmless Brainlab from all actions, including claims, demands, suits, or proceedings made or brought against Brainlab by third parties resulting from an infringement of their rights by any of Your actions or omissions, including but not limited to the disclosure of user data or patient data. You assume all reasonable attorneys' fees, costs, and expenses incurred due to an infringement of third party rights. All other rights, including but not limited to damage claims by Brainlab, shall remain unaffected.

12.4 QUENTRY IS NOT A PLATFORM DEVELOPED FOR DATA BACKUP AND DOES NOT SUBSTITUTE ANY BACKUP OR STORAGE SYSTEM FOR ELECTRONIC DATA. IT IS WITHIN YOUR RESPONSIBILITY TO KEEP BACKUPS OF ANY AND ALL OF YOUR DATA INCLUDING PATIENT DATA. IN NO EVENT SHALL BRAINLAB BE LIABLE FOR ANY LOSS OR DAMAGE OF ANY DATA.

12.5 UPON TERMINATION OR INACTIVATION OF YOUR MEMBERSHIP, EITHER BY YOU OR BRAINLAB, PATIENT DATA THAT HAS BEEN ONCE TRANSFERRED BY YOU WILL BE PERMANENTLY AND IRREVOCABLY DELETED. IN SUCH EVENT, BRAINLAB SHALL NOT BE LIABLE FOR ANY LOSS OR DAMAGE OF DATA.

13. Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND EXCEPT AS OTHERWISE EXPRESSLY SET FORTH HEREIN, BRAINLAB MAKES NO WARRANTIES, GUARANTEES OR REPRESENTATIONS OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE OPERATION, CAPACITY, SPEED, FUNCTIONALITY, QUALIFICATIONS OR CAPABILITIES OF QUENTRY OR ANY GOODS OR PERSONNEL RESOURCES PROVIDED HEREUNDER, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY OF FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT.

BRAINLAB DOES NOT WARRANT ANY PARTICULAR RESULTS THAT MAY BE OBTAINED BY THE USE OF QUENTRY OR THAT THE SERVICES OR ASSOCIATED SYSTEMS WILL

OPERATE IN AN ERROR-FREE OR UNINTERRUPTED MANNER, OR IN COMBINATION WITH THIRD PARTY PRODUCTS.

14. Data Protection

14.1 Brainlab recognizes that any data provided by You to Quentry may be important to You and requires safe and secure data handling. Brainlab shall comply with applicable legal provisions regarding data protection. In particular, Brainlab shall not provide or otherwise disclose any personally identifiable information of You to any third party without authorization. Details are given in the Quentry Privacy Policy.

14.2 If Brainlab is required to disclose any data provided by or belonging to You by a court order, an order of any public authority, or by law, Brainlab shall give immediate notice thereof to You. In the event that Brainlab is required to disclose data to which Brainlab has no access rights, You shall assist and cooperate with Brainlab in order to follow and comply with any of such requirements.

14.3 If You practice medicine in the USA or if You change the country where You practice medicine to the USA at a later time, You are required to accept the Business Associate Agreement attached as Exhibit 1: Business Associate Agreement ("BAA"). Any of Your protected health information, as such term is defined in the Health Insurance Portability and Accountability Act (HIPAA), shall only be used or disclosed as set forth in the BAA. If You are unsure whether the BAA is applicable for You, You must contact Brainlab.

14.4 According to European data protection laws and the fact that some of the processing activities may occur within the European Union (e.g. data access for support reasons) the parties are required to enter into a separate data processing agreement according to the General Data Protection Regulation (GDPR). For that purpose You accept during the registration the terms of such data processing agreement accordingly (Exhibit 2).

15. Compliance with Law

Quentry is provided solely for lawful purposes and use. Without limiting the other Terms, You agree to be solely responsible to comply with all laws, statutes, ordinances and/or regulations (including without limitation the laws and regulations governing export control, unfair competition, anti-discrimination, false advertising, privacy and data protection, and publicity) (collectively, "Laws") applicable to You and Your business and Your use of the Services. You will not directly or indirectly ship, transfer, export or transmit the Services into any country or permit or authorize use by any person in any manner prohibited by export laws, restrictions, or regulations of any applicable jurisdiction. The parties agree that Brainlab may in its sole discretion make changes to any of the Services from time to time as may be reasonably necessary or appropriate for Brainlab to comply with applicable Laws.

16. Notices

16.1 By providing us with Your email address, You agree to receive all required notices electronically by using that email address. It is Your responsibility to update or change Your email address as appropriate.

16.2 Notices to You will be provided by email or as notification within Quentry.

16.3 Unless otherwise stated, Your notices to Brainlab shall be send by email to legal@quentry.com.

17. General Provisions

17.1 This Agreement shall be governed by the laws of the Federal Republic of Germany excluding conflict of laws provisions.

17.2 Exclusive place of jurisdiction shall be Munich, Germany.

17.3 You may not assign any of Your rights or obligations hereunder, whether by

operation of law or otherwise, without the prior written consent of Brainlab. Notwithstanding the foregoing, to the extent permitted by law, Brainlab may assign rights and obligations relating to Quentry in whole or in part, without Your consent , to its affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets not involving a direct competitor of You. Subject to the foregoing, these Terms shall bind and inure to the benefit of the parties, their respective successors and permitted assigns.

17.4 In case any of the provisions of these Terms shall be held to be invalid or unenforceable in any respect, the remaining provisions shall remain in full force and effect. The invalid clause shall be replaced by such valid clause which comes closest to the commercial intention of the parties.

Exhibit 1: Quentry.com Business Associate Agreement

LAST UPDATED ON May 24, 2018

THIS Business Associate Agreement

(this "BAA") is made and entered into by and between you, as a user of Quentry ("You", "Your" or "Covered Entity") and Brainlab AG ("Brainlab" or "Business Associate"). By accepting this BAA, You agree to the terms of this BAA.

WHEREAS,

in connection with the use of the services available at Quentry.com, and all sub domains ("Services") subject to the Terms of Use and the Quentry Privacy Policy, Business Associate performs services for or on behalf of You ("Services");

WHEREAS,

the parties acknowledge and agree that You are a "Covered Entity" and Brainlab is a "Business Associate" of You when Business Associate uses and discloses Protected Health Information ("PHI") received from or on behalf of You in connection with performing the Services for or on behalf of You; and

WHEREAS,

Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI disclosed to Business Associate pursuant to this BAA in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), and regulations promulgated thereunder by the U.S. Department of Health and Human Services including the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164 of the Code of Federal Regulations, Subpart A & E ("Privacy Rule"), the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A & C ("Security Rule"), the requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 and the implementing regulations, as issued and amended by the Secretary ("HITECH").

NOW, THEREFORE, for good and valuable consideration, the receipt and adequacy of which are hereby acknowledged, You and Brainlab agree as follows:

1. Definitions.

Capitalized terms used herein without definition in this BAA shall have the respective meanings assigned to such terms by HIPAA.

2. Effect.

The provisions of this BAA shall control with respect to PHI that Business Associate receives from or on behalf of Covered Entity.

3. Obligations of Business Associate.

Business Associate shall maintain the confidentiality and security of such PHI as required of Business Associate by applicable laws and regulations, including HIPAA. Business Associate covenants and agrees to the following:

3.1 Safeguards.

Business Associate shall use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI, to prevent the use or disclosure of PHI for purposes other than those permitted in Section 4 of this BAA.

3.2 Reporting.

(a) If Business Associate becomes aware of a use or disclosure of PHI in violation of this BAA by Business Associate or by a third party to which Business Associate disclosed PHI, Business Associate shall report any such use or disclosure to Covered Entity without unreasonable delay.

(b) Business Associate shall report any successful Security Incident involving PHI of which it becomes aware to Covered Entity in writing without unreasonable delay [and if practicable within thirty (30) business days]. The parties acknowledge and agree that this section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Covered Entity shall be required. "Unsuccessful Security Incidents" shall include, but not be limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI.

(c) Business Associate shall, following the discovery of a Breach of Unsecured PHI, notify the Covered Entity of such Breach in accordance with 45 C.F.R. § 164.410 without unreasonable delay, but in no case later than sixty (60) days after discovery of the Breach.

4. Permissible Uses and Disclosures of PHI.

4.1 Use and Disclosure by Business Associate Generally.

Business Associate may use and/or disclose PHI received from or on behalf of Covered Entity, as permitted or required to perform the Services, as permitted by this BAA, and/or as Required by Law, but it shall not otherwise use or disclose any PHI. Business Associate shall not use or disclose PHI in a manner that would be in violation of HIPAA if done by Covered Entity. Business Associate is permitted to use or disclose PHI as set forth below:

(a) Business Associate may use PHI internally for its proper management and administrative services or to carry out its legal responsibilities, and as authorized by Covered Entity to perform the Services and this BAA;

(b) Business Associate may disclose PHI to a third party for Business Associate's proper management and administration or to carry out its legal responsibilities, provided that the disclosure is Required by Law or Business Associate obtains reasonable assurances from the third party to whom the PHI is to be disclosed that the third party will (1) protect the confidentiality of the PHI, (2) only use or further disclose the PHI as Required by Law or for the purpose for which the PHI was disclosed to the third party, and (3) notify Business Associate of any instances of which the person is aware in which the confidentiality of the PHI has been breached;

(c) Business Associate may use PHI to provide data aggregation services relating to the health care operations of Covered Entity; and

(d) Business Associate may de-identify PHI, consistent with applicable HIPAA requirements.

4.2 Disclosure to Third Parties.

Business Associate may disclose PHI of Covered Entity that is created or received by Business Associate on behalf of Covered Entity under this BAA to agents and subcontractors Business Associate retains to assist it in the performance of the Services to Covered Entity if and only if all such agents and subcontractors agree to the same or similar requirements and restrictions with respect to the PHI as are set forth herein. Business Associate shall ensure that any such agent or subcontractor to whom it discloses electronic PHI agrees to implement reasonable and appropriate safeguards to protect such information in compliance with HIPAA.

5. Patient Rights With Respect To PHI.

5.1 Access to Information.

Within fifteen (15) business days of a written request by Covered Entity for access to PHI about an Individual contained in any Designated Record Set of Covered Entity maintained by Business Associate, if any, Business Associate shall make available to Covered Entity such PHI for so long as Business Associate maintains such information in the Designated Record Set. If Business Associate receives a request for access to PHI directly from an Individual, Business Associate shall direct the Individual to contact Covered Entity directly.

5.2 Availability of PHI for Amendment.

Within fifteen (15) business days of receipt of a written request from Covered Entity for the amendment of an Individual's PHI contained in any Designated Record Set of Covered Entity maintained by Business Associate, if any, Business Associate shall provide such information to Covered Entity for amendment and incorporate any such amendments in the PHI (for so long as Business Associate maintains such information in the Designated Record Set) as required by 45 C.F.R. §164.526. If Business Associate receives a request for amendment to PHI directly from an Individual, Business Associate shall direct the Individual to contact Covered Entity directly.

5.3 Accounting of Disclosures.

Within fifteen (15) business days of written notice by Covered Entity to Business Associate that it has received a request for an accounting of disclosures of PHI (other than disclosures to which an exception to the accounting requirement applies under HIPAA), Business Associate shall make available to Covered Entity such information as is in Business Associate's possession and is required for Covered Entity to make the accounting required by 45 C.F.R. §164.528.

6. Availability of Books and Records.

Business Associate shall make Business Associate's internal practices, books and records relating to the use and disclosure of PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary of Health and Human Services for purposes of determining and facilitating Business Associate's and Covered Entity's compliance with HIPAA.

7. Obligations of Covered Entity.

7.1 Covered Entity shall not cause Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA if done directly by Covered Entity.

7.2 Covered Entity represents that, to the extent Covered Entity provides PHI to Business Associate, such PHI is the minimum necessary PHI for the accomplishment of Business Associate's purpose.

7.3 Covered Entity represents that, to the extent Covered Entity provides PHI to

Business Associate, Covered Entity has obtained the consents, authorizations and/or other forms of legal permission required under HIPAA and other applicable law.
7.4 Covered Entity shall implement reasonable and appropriate measures to ensure that PHI and electronic PHI are disclosed, provided or transmitted to Business Associate only in a secure manner including through the use of a technology or methodology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals.
7.5 Covered Entity shall indemnify and hold Business Associate, its affiliates and subsidiaries, and their respective directors, officers, employees and subcontractors harmless from and against any damages, costs, liabilities, expenses and settlement amounts incurred in connection with a breach by Covered Entity of this Section 7.

8. Termination and Expiration of BAA.

8.1 Term.

The term of this BAA shall be effective as of the date when Your membership for Quentry is activated ("Effective Date"), and shall terminate upon termination of Your membership.

8.2 Termination for Failure to Comply.

Covered Entity may terminate the Services immediately upon failure of Business Associate to cure a material breach of this BAA within 30 days of receipt of written notice to Business Associate if Covered Entity determines that Business Associate has violated a material term of this BAA. This BAA may be terminated by Business Associate upon 30 days written notice to the Covered Entity, if Business Associate believes that the requirements of any law, legislation, consent decree, judicial action, governmental regulation or agency opinion, enacted, issued, or otherwise effective after the Effective Date and applicable to the PHI or to this BAA, cannot be met by Business Associate in a commercially reasonable manner and without significant additional expense.

8.3 Return of PHI upon Termination or Expiration.

Upon termination or expiration of this BAA, Business Associate shall destroy all PHI received from, created or received by Business Associate on behalf of, Covered Entity to Covered Entity. If Business Associate reasonably determines that such destruction is not feasible, Business Associate will extend the protections of this BAA to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of such PHI infeasible.

8.4 Binding Effect.

Except as otherwise provided herein, the terms and conditions of the BAA shall remain in full force and effect following termination of the BAA.

9. Miscellaneous.

9.1 Amendment.

Upon enactment of any applicable law or regulation affecting the use or disclosure of PHI, or the publication of any interpretative policy or opinion of any government agency charged with the enforcement of any such law or regulation, Covered Entity, by written notice to Business Associate, may request amendment of this BAA in such manner as Covered Entity reasonably determines necessary to comply with such law or regulation to the extent such enactment is directly applicable and enforceable against Business Associate; provided, however, that to the extent such amendment causes Business Associate to incur a material increase in the costs associated with performance of the Services, the parties shall meet and negotiate in good faith to make any adjustments to the fees for the Services. In the event the parties, after good faith negotiations, cannot reach agreement regarding the amount of such adjustments, either party may terminate the Services by giving the other party at

least seven (7) days prior written notice of its intent to terminate.

9.2 Entire Agreement.

This BAA is the entire and sole understanding of the parties hereto with respect to the subject matter hereof, and supersedes all prior negotiations, understandings, transactions, or communication, whether oral, or written, including electronic form. If any provision or part thereof is found to be invalid, the remaining provisions shall remain in full force and effect. Any other terms or conditions contained in any other document with respect to PHI shall not apply.

9.3 Successors and Assigns.

This BAA will inure to the benefit of and be finding upon the successors and assigns of the parties. This BAA is not assignable by any party without the prior written consent of the other party. Notwithstanding the foregoing, Business Associate may assign this BAA in its entirety, without consent of the other party, to its affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets not involving a direct competitor of the other party.

9.4 No Third Party Beneficiaries.

Nothing express or implied in this BAA is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate, and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

9.5 Independent Contractors.

None of the provisions of this Agreement are intended to created, nor will they be deemed to create, any relationship between the parties other than that of independent parties contracting with each other solely for the purposes of effecting the provisions of this BAA and any other agreements between the parties evidencing their business relationship.

By accepting this BAA without raising any objection, You signify Your agreement with and understanding of the terms set forth herein.

Contacts:

If you have any questions, concerns, or suggestions regarding this BAA, please contact us at legal@quentry.com.

Exhibit 2: Data Processing Agreement

Supplemental Agreement on Data Processing on behalf of a Controller

between

You

("**Controller**")

and

Brainlab AG
Olof-Palme-Straße 9

81829 Munich
Germany

(“**Processor**”, together the “**Parties**”)

Preamble

This agreement (“Supplemental Agreement”) is an Exhibit to the General Terms and Conditions for the Use of Quentry. Quentry is a software invented by the Processor. It is indicated for image data transfer and online storage of medical images and related by medical professionals. Quentry users can exchange images and work together in virtual groups. Quentry provides medical professionals and associated team members with tools for secure online image (e.g. DICOM) storage, review, enrichment and sharing and supports doctors to build their global clinical network and provides an online community to work in virtual groups and send images and messages.

The General Terms and Conditions for the Use of Quentry regarding these activities or services shall in the following be referred to as the Master Agreement.

This Supplemental Agreement is concluded in accordance with the Master Agreement and shall align to the term of the Master Agreement. If Processor processes Personal Data of Controller as a Controller (e.g. usually applies to registered user data except as indicated below) the terms of this Supplemental Agreement shall not apply.

1. Definitions

In this agreement, the following terms shall have the following meanings:

"**Adequate Country**" shall mean any country outside of the EEA that is recognized by the European Commission as providing an adequate level of privacy protection by reason of its domestic law or of the international commitments it has entered into;

“**GDPR**” shall mean Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

“**Instruction**” shall mean written instructions by Controller on the specific handling of Personal Data (e.g. anonymisation, blocking, deletion, handing over) by Processor with regard to data protection.

“**Personal Data**”, “**Controller**”, “**Processor**”, “**process/processing**”, “**data subject**”, “**technical and organisational measures**”, “**supervisory authority**” or “**processing on behalf of a controller”** shall be interpreted in accordance with the GDPR.

2. Subject matter and responsibility

Processor processes Personal Data on behalf of Controller. Subject matter of the commissioning are activities as specified in the Master Agreement and the schedules annexed to the Master Agreement, in particular the specification of services. Within the scope of this Supplemental Agreement, Controller shall be solely responsible for compliance with the statutory provisions on data protection, in particular the lawfulness of the transfer of data to Processor and the processing of the data through Processor.

3. Specification of the commissioning, limited territoriality

3.1 Purpose, type and extent of the commissioned collection, processing and/or use of Personal Data are described in the Master Agreement to which insofar explicit reference is made.

3.2 The type of categories of the collected and/or used Personal Data as well as the category of data subjects who are subject to the handling of Personal Data under this commissioning are as follows:

Type of categories of the collected and/or used

Personal Data For registered users the following information is gathered (if and to the extent that Processor receives such data from a third entity (for example a hospital) and is processing such data on behalf of such third party entity): Last Name, First Name, User Name, Password, Email, Institution, Department, Function/Position, City, Postal Code, Country, Time Zone, Speciality, Profiling Information (e.g. profile on system use or other behaviour), Non-mandatory: Academic Title, , Street, Phone, Cell Phone, State

For Patient Data: medical images (e.g. DICOM), Dynamic Forms with Patient meta-data customized by the user that might include any patient information available to the physician, Patient information (Patient Id, Patient Full Name, Patient Date Of Birth, Patient Gender, Patient Date Of Mortality, Patient Race, Cause Of Mortality, Study Id, Study Instance Iid, Accession Number, Study Date, Study Description, Institution, Study Location, Modalities, Number Of Images, Patient Comments, Uploader Institution, Upload Date etc.), furthermore any data that the registered user uploads.

Categories of data subjects who are subjected to the handling of Personal Data

- Commercial Customers (including medical doctors or other hospital or health facility staff if such data is provided to Processor on behalf of the respective facility / instituition or other authorized third party)
- Patients of Customers

Further details are described in the Master Agreement to which insofar explicit reference is made.

4. Controller's right to issue instructions

4.1 Within the scope of the specifications set forth in this Supplemental Agreement, Controller reserves a right to issue Instructions concerning the type, extent and procedure of data processing which it may specify by issuing individual instructions. Changes of the subject matter of processing and procedures shall be jointly agreed upon and shall be documented.

4.2 Processor will inform Controller of any instruction that it deems to be in violation of data protection requirements. Processor may then postpone the execution of the relevant instruction until it is confirmed or changed by Controller.

5. Obligations of Processor

5.1 Processor shall, unless otherwise permitted by law or otherwise (e.g. data subject's consent), collect, process or use data only as commissioned by Controller and in compliance with the Instructions of Controller but, in particular, not for its own purposes. Processor will correct, delete, rectify or block the data processed on behalf of Controller only as instructed by Controller. If a data subject contacts Processor with a request for correction or deletion of its data, Processor shall forward the request to Controller.

5.2 Processing takes place on the instructions from the Controller only, unless the Processor is required to do so by European Union or Member State law to which the Processor is subject to; in such a case, the Processor shall inform the Controller of that legal requirement before

processing, unless that law prohibits such information on important grounds of public interest (cf., Art. 28 para. 3 lit. a GDPR).

5.3 Unless prohibited by applicable law or a legally-binding request of an authority, Processor shall promptly notify Controller of any request by government official, data protection supervisory authority or law enforcement authority for access to or seizure of Personal Data of the Controller as provided hereunder.

5.4 Before granting access to Personal Data, Processor will oblige persons employed in processing Personal Data on data secrecy and confidentiality and familiarize them with the provisions as set forth in the data protection obligations as applicable to Processor. Where necessary, this shall include obligating the relevant personnel on professional secrecy (if any, including derivative obligations, for example when processing data originating from hospitals or medical doctors) or the telecommunication secrecy if and to the extent that respective services have been agreed upon in the Master Agreement.

5.5 Insofar as required by statutory law, Processor will appoint a data protection officer and shall make its contact details available to Controller during the term of this Agreement.

5.6 Processor will without undue delay notify Controller of violations of Instructions or of provisions for the protection of Controller's Personal Data by Processor or a person employed by Processor.

If Personal Data have been lost, unlawfully transferred or otherwise unlawfully disclosed to third parties according to Art. 33 and 34 of the GDPR, Controller shall be informed of such incidences without undue delay. Processor shall, in consultation with Controller, take appropriate measures to safeguard the data as well as to mitigate potentially adverse consequences for the data subjects.

Furthermore, Processor shall without undue delay inform Controller of serious disruptions of the normal course of operations, any suspicions of data protection violations or other irregularities in processing the data of Controller.

Processor acknowledges that Controller is obliged to document breaches of the protection of Personal Data and, if necessary, inform the supervisory authority, respectively the data subject, on such breach. If and insofar as it has come to such breaches, Processor will assist the Controller in accordance with Art. 28 para. 3 lit. f GDPR with compliance of its reporting obligations in a proper manner to allow for the Controller to timely perform its obligations hereunder. Processor will inform the breach to the Controller and give at least the following information: (a) description of the kind of the breach, the category and the approximate amount of data subjects and datasets involved, (b) name and contact of a contact person for further information, (c) description on the probable consequences of the breach, (d) description of the taken measures in order to remedy or reduce the breach.

5.7 Processor will inform Controller of any monitoring activity of and measures taken by the supervisory authority with regard to the processing of Personal Data of Controller.

5.8 If Controller is obliged in accordance with applicable statutory data protection law to provide information on the collection, processing or use of data, Processor shall provide Controller with any and all respective information.

5.9 Processor shall monitor the compliance with obligations specified above during the execution of the commissioned data processing.

5.10 Processor shall maintain a written record of all categories of processing activities carried out on behalf of the Controller in accordance with Art. 30 para. 2 of the GDPR.

5.11 If applicable, Processor assists in accordance with Art. 28 para. 3 lit. f GDPR with the preparation of a data protection impact assessment pursuant to Art. 35 GDPR and, where appropriate, assists with the prior consultation of the supervisory authority pursuant to Art. 36 GDPR. On Controller's request, Processor shall disclose the required information and documents to Controller. The additional costs incurred by these services are to be reimbursed to the Processor.

5.12 The Processor shall implement appropriate measures in respect of data misuse, data loss and recoverability of data (e.g. by creating industry standard backups), as far as this is agreed in the Master Agreement.

6. Security of Processing

6.1 Within its scope of responsibility, Processor will set up its internal organization in accordance with all applicable data protection and data security requirements. Processor shall take, maintain and control technical and organizational measures to ensure reasonable protection of Controller's data against misuse and loss in accordance with the requirements according to applicable laws.

6.2 Processor takes all appropriate technical and organisational measures that comply with the requirements of Art. 32 GDPR, in order to ensure a level of security appropriate to the risk and assist the Controller in ensuring compliance with the obligations pursuant to Art. 32 GDPR (Art. 28 para. 3 lit. c, f GDPR).

6.3 In this connection, the Processor shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. This includes appropriate measures on e.g. entrance control, user control, access control, transmission control, input control, job control, availability control as well as separation by purpose and, inter alia as appropriate, the pseudonymization and encryption of Personal Data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.4 Annex 1 contains a description and specification of the required technical and organisational measures Processor will implement hereunder. These may be complemented by further related documentation provided by the Processor during or in the course of providing the services.

6.5 Technical and organizational measures are subject to technical progress and development. The Processor may implement adequate alternative measures. These must not, however, fall short of the level of security provided by the specified measures. Any material changes, however, must be documented.

6.6 Processor assists the Controller in accordance with Art. 28 para. 3 lit. e GDPR by appropriate technical and organisational measures, insofar as this is possible and reasonable, for the fulfilment of the Controller's obligation pursuant to Chapter III of the GDPR towards data subjects, e.g. the information to and access of the data subjects, rectification and erasure of data, restriction of processing or the right to data portability and right to object. The additional costs incurred by this assistance are to be reimbursed to the Processor.

7. Remote access

7.1 The following supplementary regulations apply to the performance of remote access if and to the extent that the processing activities concern special categories of Personal Data or Controller is subject to professional secrecy.

7.2 Remote access shall only be carried out with the consent of the respective authorised person / affected employee of the Controller, if and to the extent that access to Personal Data cannot be excluded.

7.3 The employees of the Processor shall use appropriate identification and encryption methods.

7.4 Remote access work shall be documented and recorded. The Controller is entitled to inspect inspection and maintenance work before, during and after execution while in doing so it shall follow the provisions as set forth under Section 9. In case of remote access, the Controller is entitled - as far as technically possible and feasible with regards to the nature of the services provided - to follow these from a control screen and to cancel them at any time.

7.5 Remote access to the relevant systems shall be performed on a need-to-know basis only.

7.6 Fault analysis that requires access to Personal Data, requires the prior consent of the Controller. If copied for such purposes, the Processor shall delete these copies after correction of the error, except if storage of the data is necessary for other purposes (e.g. documentation of the correctness of the performed activities). Such Personal Data may only be used for the purpose of fault analysis and may furthermore not be copied to mobile storage media (PDAs, USB memory sticks or similar devices) without appropriate encryption.

7.7 Remote access and all activities required in this context, in particular activities such as deletion, data transfer or fault analysis, shall be carried out taking into account technical and organisational measures for the protection of Personal Data.

8. Rights and obligations of Controller

8.1 Controller and Processor shall each be responsible for compliance with the respective statutory data protection law as it applies to the one or the other with regard to the Personal Data that are to be processed hereunder.

8.2 Controller shall specify the measures for returning the provided data media and/or deletion of recorded data after the termination of the commissioning by way of entering into a contract. If no specifications are issued, data shall be handed over to Controller or destroyed. Insofar as data are deleted in accordance with particular specifications, Processor shall confirm such deletion to Controller specifying the date on which such deletion has been effected.

9. Audit Rights

9.1 On request of the Controller the Processor shall provide the Controller with evidence of the implementation of the technical and organizational measures and the other obligations stated in Art. 28 GDPR.

9.2 Controller may carry out job control in consultation with the Processor, or appoint auditors to do so before the start of data processing and in a reasonable manner throughout the term of the commission. The Processor may comply with such requests by providing Controller at any time before the start of and throughout the term of the processing with respective self-audits, up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, the data protection officer, the IT security department, data protection or quality auditors) or suitable certification by way of an IT security or data protection audit.

9.3 If the Controller has reasonable doubts regarding the self-audit or evaluation provided by the Processor and provides the Processor with an explanation of such doubts, Controller shall be

entitled, at its on own expenses, to carry out a reasonable check on the Processor's business premises in order and insofar as to verify the implementation of the technical and organizational measures and the other obligations stated in Art. 28 GDPR. Such audit shall be announced at least two weeks in advance, only be performed during regular business hours and shall not disturb internal operations. Controller shall remunerate any additional costs incurred by Processor due to such audit.

9.4 Upon Controller's written request Processor shall provide Controller within a reasonable period of time any information and make the documentation available as necessary for the auditing.

10. Sub-Processors

10.1 Processor shall be entitled to use subcontractors and other companies for fulfilling its contractual obligations.

10.2 Processor shall ensure by entering into agreements with sub-processors to impose at least substantially the same obligations on sub-processors which Processor has assumed according to this Supplemental Agreement prior to sub-processor being granted access to Controller's Personal Data during performance. If the subcontractor provides the agreed service outside the EU/EEA and an Adequate Country, the Processor shall provide for compliance with EU Data Protection Regulations by appropriate measures.

10.3 Upon request, Processor shall provide a list of sub-processors involved in the data processing activities hereunder. Processor shall inform the Controller of any intended changes concerning the addition or replacement of other sub-processors, thereby giving the Controller the opportunity to object to such changes, whereas Controller has to present reasonable grounds for such an objection. If Controller still does not approve of a new sub-processor, then Controller and/or Processor may terminate the affected parts of the services without penalty by providing, before the end of any applicable notice period, written notice of termination.

10.4 Controller shall be entitled to auditing Processor's sub-processors in accordance to Section 9 above and upon prior consultation and agreement with Processor to that effect, whereas Controller herewith commissions Processor with executing such audits on Controller's behalf and agrees that such audit may only be executed by Processor and may also be satisfied by presenting up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, the data protection officer, the IT security department, data protection or quality auditors) or suitable certification by way of an IT security or data protection audit. Controller achknowledges that it may have to exedcute one or more confidentiality agreements with processor and/or its subprocessor before receiving respective documents and information.

10.5 Approval requirements for subcontracting shall not apply in cases where Processor subcontracts ancillary services to third parties; such ancillary services shall include, but not be limited to mail, shipping and receiving services and caretaking services.

11. Territory

11.1 As a general rule, the processing shall occur in a member state of the European Union, in a country of the European Economic Area or in an Adequate Country. Processing activities in another country ("**Third Country**") shall be allowed if the applicable requirements for international transfer of Personal Data according to Art. 44 ff. GDPR are complied with.

11.2 If and to the extent that (i) Controller and Processor are located within the Economic European Area ("**EEA**") while the sub-processor is located in a Third Country and (ii) Processor will enter into agreements with sub-processors based on the EU Standard Contractual Clauses

for Processors ("**SCC**"), Controller herewith authorizes Processor to enter into such sub-processing agreements with sub-processors. Upon request, Processor shall inform Controller on the existence and status of such Standard Contractual Clauses Agreements entered into under the above circumstances.

12. Liability

12.1 Controller shall defend and hold harmless Processor from any third party claim or other losses or liabilities arising from the other Controller's breach of his obligations hereunder and/or other violations of applicable data protection laws, unless Controller is not responsible for such third party claim or other losses or liabilities.

12.2 The liability of the Processor is limited to a 100% of the revenue received from Controller within the past 12 months preceeding the claim triggering event.

12.3 The provisions in the Master Agreement adressing liability or indemnification obligations shall other then regulated herein remain unaffected.

13. Confidentiality

The Parties shall undertake to treat as confidential any knowledge of operational and trade secrets acquired within the scope of the contractual relationship. This shall continue to apply beyond the end of individual orders and/or the business relationship.

14. Duty to inform, written form requirement, choice of law

14.1 If there is a risk that Personal Data of Controller becomes the subject of attachment or seizure, insolvency or settlement proceedings or other incidences or third party measures at Processor, Processor shall immediately notify Controller thereof. Processor will inform all persons responsible in this context, that exclusive authority to dispose and ownership with regard to the data lies with Controller.

14.2 Modifications and amendments of this Supplemental Agreement are only effective if made in written form and if explicit reference is made to the fact that this Supplemental Agreement shall thereby be modified or amended. This shall apply accordingly to a deviation from this form requirement.

14.3 This Supplemental Agreement and all legal disputes arising in connection with its taking effect or its performance shall be exclusively subject to German law excluding the Vienna Convention of the United Nations Convention on Contracts for the International Sale of Goods of April 11, 1980 (CISG). Place of jurisdiction for any disputes between the Parties in connection with this Supplemental Agreement shall be the regional court of Munich I.

Annex 1: **Security of the processing**

This Appendix describes the technical and organizational measures (TOMs) and procedures that Processor shall, as a minimum, maintain to protect the security of Personal Data created, collected, received, or otherwise obtained and ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

I. Confidentiality, Art. 32 para. 1 lit. b) GDPR

1. Physical Access Control

   The Contractor and involved cloud platform providers take in particular the following measures to prevent unauthorized persons from gaining access to data processing systems for Processing or using Personal Data:
   The physical access to the Contractor's premises including the data centers is ruled through formal access
   procedures. The access to Contractor's premises or data centers and restricted zones respectively requires proper identification and is limited to authorized personnel based on job function. Visitors have to register in a visitor's log sheet and have to wear a visitor's badge with temporary and restricted access rights. Visitors are escorted by security personnel. Additionally, security measures are implemented such as video-surveillance and security guard.

2. Logical Access Control
   The Contractor takes in particular the following measures to prevent data processing systems from being used
   without authorization:
   For User identification and authentication: User ID, password procedures incl. password complexity requirements,
   reset of generated initial password on first use, periodic change of password, password history controls and
   automatic blocking (e.g. password request or timeout). A Quentry User session expires automatically after a period of
   inactivity. The Quentry system is hosted on Amazon Web Services (AWS). The Contractor uses the AWS Identity and
   Access Management to ensure that only specifically appointed and authorized employees of the Contractor have
   access to the Quentry system for support and maintenance. All Users with elevated access rights will be required to
   use AWS Multi-Factor Authentication. On network level the AWS Security Groups (firewall) are configured to restrict
   administrative access to the Quentry system only to inbound connections from the secured network of the Contractor.
   AWS is utilized for User authentication (storage of User name and password). The network connection from the Quentry system to the AWS system is encrypted via SSL. The passwords are stored encrypted.

3. Data Access Control

The Contractor takes in particular the following measures to ensure that persons authorised to use data processing
systems have access only to those data they are authorized to access, and that Personal Data cannot be read,
copied, altered or removed without authorization during Processing, Use and after recording:
Administrative access to the Quentry system and stored Personal Data is granted for a very limited number of
employees of the Contractor. The assigned authorizations are based upon job responsibilities and provisioned to
least privilege. Such access is granted to restart the Services and any other activity to maintain a secure and
operational Quentry system. Remote access is configured in the firewall (AWS security group) to allow access only
from the Contractor's network.
All processed files are stored encrypted either with the Advanced Encryption Standard (AES 256) or using BitLocker
Drive Encryption. The corresponding encryption key is stored encrypted on another virtual machine. As only the
Contractor processes the encryption keys, cloud platform providers do not have access to view decrypted data. A
multi-tenant system is employed which ensures that a User cannot access Personal Data of another User unless the
other User gives the approval through setting granular sharing permissions via the Quentry system.

4. Separation Control

The Contractor takes in particular the following measures to ensure that data collected for different purposes can be
processed separately:
Client's Personal Data is processed on server systems, which are logically separated within the network. A strong
logical separation of Client data is achieved via client-specific User IDs that permits only authorized Users to view
related Client data. Client may implement a granular sharing model and User permission profiles to limit data access to different Users.

II. Pseudonymisation and Encryption, Art. 32 para. 1 lit. a) GDPR

Measures for the pseudonymisation and encryption of personal data (if not already mentioned in section I.):
As part of the service Quentry offers the option to remove patient information from DICOM images during upload, before sharing such de-identified data with other Quentry users. Users must confirm that all visible patient information has been removed from the selected data.

III. Integrity, Art. 32 para. 1 lit. b) GDPR

1. Data Transfer Control

   The Contractor takes in particular the following measures to ensure that Personal Data cannot be read, copied,
   altered or removed without authorization during electronic transfer or transport or while being recorded onto data
   storage media, and that it is possible to ascertain and check to which parties Personal Data is transferred to:
   The communication between the User client and the Quentry system is secured through SSL certificate (issued by
   GlobalSign, minimum 128-bit to 256-bit encryption, depending on client capabilities) and a session ID generated by
   the Quentry system. The session ID is created during the login process and is only valid for the period the User is
   active.

2. Data Entry Control

   The Contractor takes in particular the following measures to ensure that it is possible after the fact to check and
   ascertain whether Personal Data have been entered into, altered or removed from data processing systems and if so,
   by whom:
   An event log is implemented tracking the Use of the Quentry system by the User. The log documents access and Use
   of Quentry containing Client data, including the access ID, time, authorisation granted or denied, and relevant activity.

IV. Availability and Resilience, Art. 32 para. 1 lit. b) und c) GDPR

   The Contractor takes in particular the following measures to ensure that Personal Data are protected against
   accidental destruction or loss:
   The Contractor uses a combination of redundant systems, firewall, anti-virus solution, intrusion detection system and
   data security as well as backup solution, to protect - and if necessary restore - the Client's Personal Data. A backup
   and disaster recovery concept describing the relevant procedures as well as responsibilities of personnel is in place.
   Disaster recovery is tested regularly.

V. Process for regularly Testing and Evaluating, Art. 32 para. 1 lit. d) GDPR

1. Data Protection Management

   Other measures, in particular organizational measures to protect Personal Data include the appointment of a data protection officer. The data protection officer is involved in relevant data

processing activities. Further, regular testing of data protection measures is executed. Data protection regulations are described in binding guidelines and instructions. Up-to-date information on IT security and IT vulnerabilities is obtained.

2. Incident Response Management

Other measures for managing data protection incidents encompass policies for data privacy and IT security, including incident reporting process, as well as business continuity management processes.

3. Privacy by Default, Art. 25 para. 2 DSGVO

Measures to ensure that pre-settings meet the interests of the data subjects (privacy by default): Images, attached documents, and comments are only viewable by the individual user and those contacts which have been granted access to the specific patient folder. Quentry users are able to define specific data handling permissions for each contact with whom they share patient information. Users define permissions for tasks including viewing, downloading, and uploading additional medical data. Further, privacy hints are provided to users with additional information on data privacy with Quentry.

4. Order Control

The Contractor takes in particular the following measures to ensure that Personal Data processed on behalf of the
Client is processed in compliance with Client's instructions:
As set forth in the Data Processing Agreement, the Contractor shall process Personal Data of the Client in accordance with the instructions of the Client. Records of processing activities are maintained. Staff of contractor is regularly trained on data protection. Prior to the commencement of Processing, and in regular intervals thereafter the Contractor monitors the technical and organizational measures taken by subcontractors.