



Data Processing Agreement

Provisions on the disclosure and processing of patient data

Status June 2026

Preamble

The Client uses a system provided by or acquired from LAP in the field of radiotherapy ("System"). The System also records health data of the patients treated by the Client ("patient data"). The Patient Data remains in the Client's IT infrastructure. The System does not transmit Patient Data to LAP, nor does LAP have access to this data during normal operation of the System.

In the case of installation, maintenance, support or other services, however, it is possible that LAP may gain access to Patient Data or that Patient Data may be transferred to LAP.

All obligations described in this Agreement apply to all activities in which employees of LAP or third parties commissioned by LAP come or may come into contact with Patient Data or other personal data (hereinafter collectively referred to as "personal data") of the Client.

This Agreement takes into consideration the requirements of the EU General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Privacy Rule, the US Security Rule, the US Breach Notification Rule and US Enforcement Rule as well as the Personal Information Protection Law of the People's Republic of China ("PIPL").

For US Clients, this Agreement serves as Business Associate Agreement, with LAP being the Business Associate and the Client being the Covered Entity, each as defined by HIPAA.

Where personal data from Chinese Clients is processed by Contractor, the standard contract for cross-border transfer of personal information as formulated by the Cyberspace Administration of China shall apply in addition to this agreement, available under www.lap-laser.com/data-processing/.

§ 1 Subject Matter

(1) LAP may provide the following services in particular if so instructed by the Client:

Purpose of data processing	Type of data	Circle of those affected
Installation, service, support and maintenance of the System manufactured and provided by LAP and used by the Client Training of the Client Error analysis, troubleshooting	Patient data Name, gender, age, nationality, occupation, contact information, health insurance company, patient number, insurance number, examination results, therapy measures, course of illness, treatments carried out, medical image data, any previous illnesses	Patients of the Client

§ 2 Responsibilities

- (1) The Client is the "controller" within the meaning of the data protection laws and is responsible for ensuring that (i) it has collected and may process the personal data in accordance with the applicable statutory and regulatory provisions and (ii) it protects the personal data in its infrastructure through appropriate technical and organizational measures in accordance with the applicable laws. The Client is also responsible for the secure and data protection-compliant transfer of personal data to LAP for the purpose of processing on behalf.
- (2) **The Client shall only make available to LAP or enable LAP to obtain knowledge of the personal data that is absolutely or minimally necessary for the provision of LAP's services. If anonymized or deidentified data can be used, the Client is obliged to anonymize or deidentify the personal data before making it available in accordance with the applicable data protection regulations.**
- (3) LAP is the processor. The processing of the personal data on behalf of the Client by LAP shall be carried out in accordance with the applicable statutory provisions and the provisions set out in this Agreement.
- (4) Client and LAP must ensure that its personnel authorized to process the personal data (i) are familiar with the provisions of the applicable data protection law and (ii) have undertaken in writing or in similarly authenticated form to maintain confidentiality or are subject to an appropriate statutory duty of confidentiality. Each party is responsible for its own personnel.

§ 3 Authority of the client to issue instructions

- (1) The data shall be processed exclusively within the framework of the agreements made and in accordance with the documented instructions of the Client. The responsibility for the instructions issued by the Client lies with the Client.
- (2) The Client's instructions are initially given in the underlying contract between LAP and the Client. Any further instructions must be issued by the Client in writing (at least in text form). The Client shall confirm verbal instructions immediately in writing or by e-mail (in text form).
- (3) LAP shall notify the Client immediately if, in its opinion, an instruction issued by the Client violates statutory or regulatory provisions. LAP shall be entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the Client.

§ 4 Place of performance

- (1) LAP shall provide the contractual services on-site at the Client's premises, remotely or at its registered office. LAP understands and agrees that, whether the contractual services are provided on-site at the Client's premises, remotely or at its registered office, it must comply with the applicable data protection laws.
- (2) Where a cross-border transfer of personal data is required in order to enable LAP to provide support and services for its medical devices, the Parties acknowledge and agree that the level of data protection ensured in the Federal Republic of Germany is considered equivalent to the data protection requirements applicable under the Client's respective local laws.

§ 5 Obligations of LAP

- (1) LAP may only process personal data within the scope of the contractual agreements and the Client's instructions. Processing by LAP for its own purposes is prohibited.
- (2) LAP shall comply with the requirements of the applicable data protection laws.
- (3) LAP shall design the internal organization in its area of responsibility in such a way that it meets the special requirements of data protection. It shall take appropriate technical and organizational measures to adequately secure the Client's personal data against misuse and loss in accordance with the requirements

of the relevant data protection statutes and regulations. LAP's technical and organizational measures are available under the following link www.lap-laser.com/en/data-processing. The Parties agree that these describe an appropriate level of protection. If a need for adjustment arises (e.g. due to new legal requirements), this must be implemented by mutual agreement.

- (4) The technical and organizational measures are subject to technical progress and further development. In this respect, LAP is permitted to implement alternative, adequate measures. In doing so, it must be ensured that the contractually agreed level of protection is not undercut. Significant changes must be documented.
- (5) LAP shall comply with the applicable data protection documentation obligations and shall provide the Client with the information that the Client requires to fulfill its statutory data protection documentation obligations to the best of its ability. LAP shall also provide information available to it to assist with any data protection impact assessment that may be required.
- (6) LAP shall be obliged to treat as confidential all knowledge of the Client's business secrets and data security measures obtained in the course of the contractual relationship and shall so oblige all its employees entrusted in the provision of services for the Client.
- (7) LAP has nominated a data protection officer who can be reached under datenschutz@lap-laser.com.
- (8) LAP shall inform the Client without delay of any breaches by LAP or the persons employed by LAP against data protection regulations or the stipulations made in this Agreement if personal data from the sphere of the Client is or can be affected. LAP shall take the necessary measures to secure the data and to minimize possible adverse consequences for the data subjects and shall consult with the Client immediately in this regard. LAP shall support the Client in fulfilling the information obligations vis-à-vis the competent supervisory authority or those affected by a personal data breach.
- (9) If a data subject contacts LAP directly to request the correction or deletion of their data, LAP shall forward this request to the Client without delay and shall support the Client in fulfilling the data subject's rights in a reasonable manner.
- (10) If the Client is obliged under applicable data protection laws to provide a data subject with information on the processing of that person's data, LAP shall support the Client in providing this information.
- (11) LAP shall inform the Client immediately of any controls and measures carried out by the supervisory authorities or if a supervisory authority investigates LAP if the Client's personal data is or could be affected.
- (12) Should the Client's personal data be jeopardized by seizure or confiscation, by insolvency or composition proceedings or by other events or measures of third parties, LAP shall inform the Client thereof without delay. LAP shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the Client as the responsible person. Nevertheless, it shall be the sole burden of the Client to take action to regain control and possession of its personal data.
- (13) If LAP is obliged by the law applicable to it to process the personal data in another way, LAP shall notify the Client of these legal requirements prior to processing. The notification shall not be made if the relevant national law prohibits such notification due to an important public interest.

§ 6 Special provisions for processing of patient data

- (1) In the provision of services on the System, LAP may gain access to patient data stored on the Client's system. The Client undertakes to provide LAP with knowledge of patient data only to the extent that this is absolutely necessary for the performance of the assigned services. The Client shall take appropriate measures to prevent LAP from gaining knowledge of patient data that go beyond this. LAP undertakes to maintain confidentiality regarding patient data and to obtain knowledge of such data only to the extent that this is necessary for the fulfilment of the tasks assigned to it.
- (2) LAP shall ensure that all employees involved in the processing of patient data and other persons working for LAP who are involved in this have undertaken in text form to maintain confidentiality about the patient data that becomes known to them in the course of or on the occasion of their work (even beyond the duration of their employment) and that they have been instructed about the possible criminal liability.

- (3) For any remote access, the Parties shall use a secure remote software. If at Client's request, the Client's remote software shall be used, the Client must ensure that the software fulfils the legal requirements. Remote access shall be documented and logged. The Client is authorized and instructed - as far as technically possible - to track remote access at any time. The Client also has the option of cancelling or preventing remote access at any time.
- (4) **The Client shall only grant LAP the access rights required for the performance of the services (also for a limited period of time) and shall ensure that LAP is not exposed to patient data that is not absolutely necessary for the execution of the services. Whenever possible, the Client shall anonymize patient data prior transferring it to LAP.** LAP shall only make use of the access rights granted to it to the System to the extent - also in terms of time - that is necessary for the proper execution of the commissioned services.
- (5) Activities for error analysis that require data transfer to LAP are always carried out in consultation with the Client. Data transfer shall preferably take place via a secure data upload as further agreed between the Parties. LAP provides for a secure upload software named Tresorit, where the transferred data is encrypted during transit and at rest.
- (6) If patient data is transferred via external data carriers of the Client, the Client shall be responsible for the protection of the data carriers provided (e.g. by encryption / password protection). The data carriers must be stored carefully by LAP so that they are not accessible to third parties. Patient data from the sphere of the Client shall not be transmitted to LAP by e-mail.
- (6) If the System is returned to LAP for maintenance, service, replacement, exchange or return, the Client must delete patient data stored on it in advance. In case that LAP receives returned devices with patient data still stored on it, LAP reserves the right to delete such data to avoid further exposure to LAP employees or third parties. The Client must ensure that the patient data are properly stored or archived elsewhere and that deletion of the patient data from the System by LAP does not lead to permanent deletion of the patient data. LAP is not responsible for the availability of patient data.
- (7) Should LAP receive requests - including in the case of interrogations and questioning by courts, public prosecutors' offices, police stations or other authorities - to disclose, pass on or otherwise use Client's patient data, the Client must be informed of this immediately and its consent obtained in advance. Only the Client is entitled to release LAP from the obligation of confidentiality or to authorize the release of the data. In the event of confiscation, LAP shall object to this and inform the Client immediately.

§ 7 Obligations of the Client

- (1) The Client is solely responsible for assessing the permissibility of the data processing and for safeguarding the rights of the data subjects. The Client shall ensure in its area of responsibility that the legally required conditions for data collection and data processing (e.g. by obtaining declarations of consent for the processing of the data) are fulfilled so that LAP can provide the agreed services without infringing the law.
- (2) The Client must inform LAP immediately and if it discovers errors or irregularities in the data processing by LAP.
- (3) The Client is obliged to inform (i) the controlling governmental, regulator or supervisory authority if the client's personal data is affected and (ii) the data subjects affected by a personal data breach.
- (4) The Client shall stipulate the measures for the return of the data carriers provided and/or the deletion of the stored data after completion of the order by contract or by instruction.
- (5) The Client is obliged to treat all knowledge of LAP's trade secrets and data security measures obtained in the course of the contractual relationship as confidential.
- (6) The Client shall ensure that it also takes appropriate technical and organizational measures to protect the data and that it complies with these measures. This applies in particular if Client provides remote access to LAP.

- (7) If the Client issues individual instructions that go beyond the contractually agreed scope of services, the resulting costs shall be borne by the Client. If the agreed scope of services is exceeded, a separate written agreement must be made in advance.

§ 8 Control rights of the Client

- (1) The Client is entitled, after timely notification during normal business hours and without disrupting operations, to inspect LAP's compliance with the applicable statutes and regulations and this Agreement in person or through a competent third party who may not be in a competitive relationship with LAP.
- (2) If LAP or the persons employed by LAP violate data processing regulations, the Client's instructions or the provisions of this Agreement, a related inspection may also be carried out without timely notification.
- (3) LAP shall support the Client in carrying out the aforementioned inspection and shall provide it with all information required to carry out an inspection within a reasonable period of time upon written request.

§ 9 Deletion of data and data carriers

- (1) Once the processing services have been completed, LAP shall delete all personal data in accordance with the applicable data protection statutes and regulations; the return of the data to the Client must be agreed in advance. Exceptions exist if LAP is legally obliged to maintain or store the personal data. In this case, the provisions of this Agreement for the protection of personal data shall continue to apply until the final deletion / handover.
- (2) Confirmations / proof of the deletion of the Client's personal data in compliance with data protection regulations will be made available to the Client on request.
- (3) LAP is not obliged to store and maintain the Client's personal data. LAP only receives patient data for support and service purposes and will delete patient data afterwards. Availability of patient data is always the sole responsibility of Client.

§ 10 Subcontractors

- (1) LAP is entitled to engage qualified sub-contractors in the provision of the services, especially its affiliated companies. These may be located in different geographic regions in order to offer service availability across multiple time-zones.
- (2) Where LAP engages an affiliated company with the provision of services, no separate consent of the Client is required.
- (3) In case that a transfer of patient data to LAP is required, the Client acknowledges that this transfer will take place to LAP GmbH Laser Applikationen, located in Germany which is the manufacturer of the System.
- (4) LAP shall ensure that the sub-contractor complies with the provisions set out in this Agreement and has an adequate level of protection to protect the Client's personal data. LAP shall also ensure that the legal requirements for the transfer of personal data to the sub-contractor, if required, are met. LAP shall bear full supervisory responsibility for the data processing activities of subcontracted entrusted parties.

§ 11 Right of retention

The defense of the right of retention, regardless of the legal grounds, to the personal Data from the Client's sphere is excluded.

§ 12 Liability

- (1) The Client and LAP are jointly liable to the data subject for any damage caused by any non-compliance in the processing of its personal data due with the applicable data protection regulations.

- (2) If a party has paid full compensation to an affected person, it shall be entitled to recover from the other party that part of the compensation which corresponds to its share of responsibility for the damage.
- (3) LAP shall be liable in the internal relationship exclusively for damage resulting from processing carried out by it in which
 - a. LAP has not complied with the obligations arising from the data protection laws applicable to it and specifically imposed on processors, or
 - b. LAP acted in disregard of the lawfully issued instructions of the Client or
 - c. LAP has acted contrary to the lawful instructions of the Client.

Further liability claims under the applicable laws remain unaffected.

§ 13 Inclusion and amendments

This Agreement shall apply to all orders that involve the processing of personal data from the sphere of the Client by LAP. Any amendments and supplements require a written agreement and an express reference to the fact that these provisions are being amended or supplemented (electronic signature is sufficient).

§ 14 Severability clause

- (1) Should individual provisions of this Agreement prove to be invalid or unenforceable in whole or in part or become invalid or unenforceable as a result of changes in legislation after conclusion of the Agreement, this shall not affect the remaining provisions of the Agreement and the validity of the Agreement as a whole.
- (2) The invalid or unenforceable provision shall be replaced by a valid and enforceable provision that comes as close as possible to the meaning and purpose of the invalid provision.
- (3) If the Agreement proves to be incomplete, the provisions that correspond to the meaning and purpose of the contract and would have been agreed in the event of consideration shall be deemed to have been agreed.
- (4) If there are several effective and enforceable provisions that can replace the ineffective provision referred to in Section 11 (1), the provision that best guarantees the protection of personal data within the meaning of this contract must be selected.

§ 15 Choice of law, place of jurisdiction

- (1) The place of jurisdiction for any disputes arising from and in connection with this Agreement shall be the place of business of the commissioned LAP entity. The law of the place of business LAP shall apply to the exclusion of the conflict of laws rules.
- (2) If a different law / place of jurisdiction is mandatory under local law (e.g. in the case of claims by data subjects), the law and place of jurisdiction prescribed by law shall apply.