LICENSE AGREEMENT

This License Agreement ("**Agreement**") governs your engagement with NovaSight Ltd. ("**NovaSight**", "**Company**", "**we**," "**us**" or "**our**"), with respect to your access to, interaction with or use of the NovaSight's CureSight™ visual system, providing eye tracking based amblyopia treatment ("**System**"), supported by a cloud-based platform which processes the data directly from the System ("**Platform**").

This Agreement is a legally binding and enforceable agreement between you (collectively referred to herein as "**you**" or "**your**"):

(i) NovaSight's customers that are Eye Care Providers who use the Platform ("**ECPs**" or "**Customer**"); and

(ii) Customer's patients, who are the children that use the System and their legal guardian ("**Patient**"),

and NovaSight (regardless whether a Patient acquired the System independently or through its health insurance company. You and NovaSight shall each be referred to herein as a "**party**" and collectively as the "**parties**".

ACCEPTANCE OF THE AGREEMENT: BY REGISTERING TO USE THE SERVICES, OR BY OTHERWISE USING THE SYSTEM AND/OR THE PLATFORM, YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTOOD AND AGREED TO THE TERMS OF THIS AGREEMENT. YOU AGREE TO BE BOUND BY THIS AGREEMENT AND TO COMPLY WITH ALL APPLICABLE LAWS AND REGULATIONS REGARDING YOUR USE OF THE SERVICES. IF YOU DO NOT AGREE TO ALL OR PART OF THIS AGREEMENT PLEASE DO NOT REGISTER OR USE THE SERVICES IN ANY MANNER.

1. REGISTRATION AND ACCOUNT

1.1 In order to use the Platform, a Customer must first provide his details in order to create an account ("**Customer's Account**"). The Customer will be required to provide his/her full name, a valid email address, phone number, its profession, all as part of the registration process. Once the registration process is complete the Customer will receive a registration confirmation email and credentials and will need to set its password, after which it will receive a confirmation that its password has been saved. The Customer hereby represents and warrants that he/she will provide accurate and complete information in connection with the Customer Account. NovaSight reserves the right to suspend or terminate the Customer Account in the event that the Customer has provided it with any untrue or inaccurate information. The Customer may not assign or transfer his/her rights under the Customer Account, including his/her username and password, without the prior written direct consent of NovaSight or its authorized representatives, provided however that each credential might be used also by the Customer's clinic in compliance with the terms of the Agreement. The Customer may update and revise some of the information that is included in the Customer Account from time to time.

1.2 Following the fulfillment of the registration process by the Customer, to our sole satisfaction, and in order to access to and interact with the System, the legal guardian will provide its contact details in order to receive a designated username and password to enter the Patient's account ("**Patient Account**" and collectively with the Customer Account "**Account**").

1.3 Each the Customer, the Guardian and the Patient shall be fully responsible to maintain the confidentiality of your username and password and for all activities occurred under your Account, whether done by you or on your behalf. Any unauthorized use or access to your Account must be immediately reported to NovaSight and its authorized representatives, where applicable.

2. SCOPE OF SERVICE

2.1 Subject to the terms herein, once you have completed the registration process or were provided with your designated log-in credentials, you will receive direct access to the System and/or the Platform, according to your interaction with us. NovaSight hereby grants you a limited, revocable, non-exclusive, non-transferable and non-sub-licensable license to access and use the System or Platform, as applicable, solely during the Term (as defined below) and solely for the purpose set forth herein ("**License**").

2.2 NovaSight, at its sole discretion, is entitled to: (i) determine the features, settings, or other tools which are available as a part of the System and/or the Platform; (ii) modify, correct, amend, update, upgrade, enhance, improve, remove, replace or make any other changes to, or discontinue, or cease, temporarily or permanently, any features or functionalities of the System and/or the Platform; and (iii) modify and renew the license under any of the circumstances listed in (ii) above, without incurring any liability to you.

3. LICENSE RESTRICTIONS

3.1 You hereby undertake that you will not, and not allow others to: (i) sell, license (or sub-license), lease, assign, transfer, pledge, or share the License granted or any rights under this Agreement with any third party except as permitted hereunder; (ii) disassemble, decompile, reverse engineer or attempt to discover the System's source code or underlying algorithms; (iii) upload invalid data, viruses, worms, malicious code or other software agents through the System and/or the Platform; (iv) interfere with the proper working or security measures of the System and/or the Platform; (v) bypass the measures NovaSight may use to prevent or restrict access to the System and/or the Platform; (vi) use the System and/or the Platform for any illegal or unauthorized purpose, or that could give rise to any civil liability or other lawsuit; (vii) modify the System and/or the Platform, or insert any code or product, or in any other way manipulate the System and/or the Platform in any way or create any derivative works from the System and/or the Platform; or (viii) use the System and/or the Platform in a manner that violates or infringes any rights of any third party, including but not limited to, privacy rights, publicity rights or intellectual property rights.

3.2 Your failure to comply with the provisions set forth above may result in, at NovaSight's sole discretion, the termination or suspension of access to the System and/or the Platform as well as the immediate termination of this Agreement, without derogating from any other remedy NovaSight may be entitled to under this Agreement or any applicable law.

4. REPRESENTATIONS AND WARRANTIES

Each party represents and warrants that it has the full legal authority to enter into and be bound by this Agreement and that it has no contractual and/or other hindrance to enter into this Agreement and to take upon itself to perform all of its undertakings hereunder.

5. TERM AND TERMINATION

5.1 This Agreement shall commence on the date you accepted its terms by accessing the System and/or the Platform, and shall thereafter continue for the duration of your use of the System and/or the Platform ("**Term**").

5.2 Notwithstanding the above, NovaSight may terminate this Agreement, for any or no reason, by providing you with a thirty (30) days prior written notice. Further, NovaSight may terminate this Agreement without any notice to you, with or without cause and immediately block access or suspend your Account, without any liability to NovaSight, if it suspects that you have breached this Agreement.

5.3 Upon the termination of the Agreement all rights and licenses granted under the Agreement shall immediately terminate and you shall cease your use of the System and/or the Platform. All sections detailed herein which by their nature are intended to survive termination, shall survive termination or expiration for any reason.

6. INTELLECTUAL PROPERTY RIGHTS

6.1 The Intellectual Property Rights and all other rights, title and interest of any nature in and to the System or any related documentation made available by or on behalf of NovaSight hereunder (including all modifications, enhancements, upgrades, customizations and derivative works thereof) are and shall remain the exclusive property of NovaSight and its licensors. For the purpose of this Agreement "**Intellectual Property Rights**" shall mean all intellectual property rights of every kind and description, including without limitation: (i) rights in or to trademarks and service marks (whether or not registered), trade names and other designations of source of origin, together with all goodwill related to the foregoing, (ii) patents and patent applications, (iii) rights in or to copyrights, whether or not registered, (iv) rights in or to trade secrets and confidential information, including without limitation know-how, technology methods, ideas and inventions, (v) rights in software and computer code (whether in source code, object code or any other form) and (vi) all applications and registrations of any of the foregoing.

6.2 If NovaSight receives any feedback (e.g., questions, comments, suggestions etc.) regarding the Platform ("**Feedback**") from the Customer, all rights, including Intellectual Property Rights in such Feedback shall belong exclusively to NovaSight and to the extent required by applicable law, the Customer hereby irrevocably transfer and assign all Intellectual Property Rights it may has in such Feedback to NovaSight and waive any and all moral rights that it may has in respect thereto.

6.3 Nothing in this Agreement shall be construed as transferring any right, title or interest to you or any third party, unless explicitly stated hereunder. NovaSight and its licensors reserve any and all rights not expressly granted in this Agreement. The provisions of this section shall remain in full force and effect after termination or expiration of the Agreement for whatever reason.

7. INDEMNIFICATION

You shall indemnify, defend and hold NovaSight harmless, and its respective affiliates, officers, directors, shareholders, or representatives ("**Indemnified Parties**") from any and all demands, judgments, awards, losses, damages, expenses, claims and liabilities, and all related costs, including reasonable legal fees ("**Liabilities**") incurred by the Indemnified Parties as a result of or arising out of a third party claim in connection with: (i) your breach of this Agreement; (ii) your gross negligence, willful misconduct or fraud, or that of your employees', agents', or subcontractors'; (iii) a medical negligence or medical malpractice caused by your actions or (iv) any breach or violation of applicable law by you.

8. LIMITATION OF LIABILITY AND DISCLAIMER

EXCEPT AS OTHERWISE EXPRESSLY STATED HEREUNDER, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SERVICES AND ANY RELATED DOCUMENTATION, SOFTWARE OR COMPONENT THEREIN ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS WITHOUT WARRANTY OF ANY KIND.

NOVASIGHT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, AND MAKES NO REPRESENTATION NOR DOES IT EXTEND ANY WARRANTY OF ANY KIND, WITH RESPECT TO THE SERVICES OR THE RESULTS AND ANALYSIS CALCULATED THROUGH THE SERVICES ("OUTPUTS"), INCLUDING WITHOUT LIMITATION WARRANTIES OF ACCURACY OR FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, TITLE, QUALITY, TIMELINESS, COMPLETENESS, OR INFORMATIONAL CONTENT. NOVASIGHT WILL HAVE NO DUTY OR OBLIGATION TO VERIFY, CORRECT, COMPLETE OR UPDATE ANY OUTPUTS OR INFORMATION DISPLAYED IN OR AVAILABLE THROUGH THE SERVICES. YOUR USE OF OR RELIANCE ON ANY OUTPUTS SHALL BE DONE SOLEY AT YOUR OWN RISK.

NOVASIGHT ASSUMES NO RESPONSIBILITY OR LIABILITY FOR: (I) ANY UNAUTHORIZED ACCESS TO OR USE OF THE ACCOUNT; (II) ANY INTERRUPTION OR CESSATION OF TRANSMISSION TO OR FROM THE SERVICES; (III) ANY BUGS, VIRUSES, TROJAN HORSES, OR THE LIKE WHICH MAY BE TRANSMITTED TO OR THROUGH THE SERVICES; AND (IV) ANY LOSS OF DATA. IN NO EVENT SHALL NOVASIGHT BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING, WITHOUT LIMITATION, INDIRECT, CONSEQUENTIAL, SPECIAL, PUNITIVE OR INCIDENTAL DAMAGES, ARISING OUT OF THE USE OF THE SERVICES, EVEN IF IT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, AND TO THE EXTENT NOT PROHIBITED BY APPLICABLE LAW, NOVASIGHT'S MAXIMUM AGGREGATE LIABILITY FOR DAMAGES IN CONNECTION WITH THIS AGREEMENT AND USE OF THE SERVICES SHALL NOT EXCEED US$100.

9. CONFIDENTIALITY

In the context of the relationship under this Agreement, the Customer and/or NovaSight ("**Disclosing Party**") may disclose to each other ("**Receiving Party**") certain confidential information regarding its technology and business ("**Confidential Information**"). The Receiving Party agrees to keep confidential and not disclose or use any Confidential Information except to support its use or provision of the services. Confidential Information shall not include information that Receiving Party can show: (i) was already lawfully known to or independently developed by Receiving Party without access to or use of Confidential Information, as evidenced by written and dated record: (ii) was received by Receiving Party from any third party without restrictions; (iii) is publicly and generally available, free of confidentiality restrictions; or (iv) is required to be disclosed by law, regulation or is requested in the context of a law enforcement investigation, provided that Receiving Party provides Disclosing Party with prompt notice of such requirement and cooperates in order to minimize such requirement. Receiving Party shall restrict disclosure of Confidential Information to those of its employees and contractors with a reasonable need to know such information and which are bound by written confidentiality obligations no less restrictive than those set out herein. The non-disclosure and non-use obligations set forth in this Section shall survive the termination or expiration of this Agreement for a period of 3 years.

10. PRIVACY AND DATA PROTECTION

10.1 NovaSight will store, process and use the information you provide during your interaction with the System and/or the Platform and use of the services, in accordance with our privacy policy.

10.2 The Customer acknowledges and agrees that NovaSight is solely a service provider. Further, as a Customer, you may grant us access or share with us certain Personal Data, Special Categories of Personal Data or Protected Health Information (as such terms are defined in **Exhibit A** and **Exhibit B** hereto) of your Patients through your use of the services. Such Personal Data, Special Categories of Personal Data or Protected Health Information shall be processed in accordance with the Data Processing Addendum attached hereto as **Exhibit A** (**"DPA"**) in the event Customer's Patients are located in the EU or the EEA, or in accordance with the Business Associate Addendum (**"BAA"**) attached hereto as **Exhibit B** in the event Customer's Patients are located in the US.

11. AMENDMENTS

NovaSight reserves the right to modify, correct, or amend this Agreement at any time. The most current version of this Agreement will always be displayed on the System and/or the Platform and any changes will be indicated under the "Last Amended" date above. It is your responsibility to ensure that you are familiar with the most current version of this Agreement. Your continued use of the System and/or the Platform following the publication by NovaSight of an amended version of this Agreement shall constitute your express agreement to be bound by the amended Agreement.

12. MISCELLANEOUS

12.1 Governing Law and Jurisdiction. This Agreement and any claim, controversy, or dispute arising out of, related to, or otherwise in connection with this Agreement shall be interpreted, construed, and enforced in accordance with the laws of the state of Israel, applied without giving effect to any conflicts of law principles. The parties agree that any lawsuit that may be brought with respect to this Agreement shall be brought and tried exclusively in the competent courts located within Tel Aviv, Israel.

12.2 Relationship of the Parties. Each party hereunder is considered an independent contractor. Nothing herein shall be deemed or construed to create a joint venture, fiduciary or agency relationship between the parties for any purpose.

12.3 Assignment. This Agreement may not be assigned or transferred by you without NovaSight's prior written consent.

12.4 Force Majeure. Neither party shall be liable for any delay or failure to perform if and to the extent that such delay or failure to perform is caused or otherwise brought about by circumstances beyond the non-performing party's reasonable control, including strikes, lockouts, labor troubles, restrictive government or judicial orders or decrees, riots, insurrection, war, terrorism, Acts of God (including a pandemic), and/or inclement weather, which the non-performing party is unable to prevent by the exercise of reasonable due diligence, and provided that the non-performing party uses its best efforts to overcome any such circumstances.

12.5 Entire Agreement. This Agreement and any links included herein, contains the entire agreement of the parties, and supersedes any prior oral or written agreements or understanding between the parties.

12.6 Severability. Should any one or more of the provisions of this Agreement be determined to be invalid, unlawful, or unenforceable in any respect, the validity, legality, and enforceability of the remaining provisions of this Agreement shall not in any way be affected or impaired by such determination and will remain in full force and effect, and the provision affected will be construed so as to be enforceable to the maximum extent permitted by law.

12.7 Waiver. Any delay or omission by either party to exercise any right under this Agreement shall not be construed to be a waiver of such right. A waiver by either party of any of the performance provisions of this Agreement shall not be construed to be a waiver of any succeeding performance or breach.

EXHIBIT A

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is executed between NovaSight Ltd. and the Customer, and reflects the parties' obligations and rights with respect to the processing of Patients' Personal Data, Special Categories of Personal Data and Protected Health Information (as such terms are defined below).

1. DEFINITIONS

1.1 **"Adequate Country**" is a country that an adequacy decision from the European Commission.

1.2 "**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. Seq.

1.3 **"Controller"**, **"Processor"**, **"Data Subject"**, **"Individual" "Personal Data"**, **"Processing"** (and **"Process"**), "**Personal Data Breach,**" **"Protected Health Information"** and **"Special Categories of Personal Data"** shall all have the meanings given to them in the EU Data Protection Law. The terms "**Personal Information**", "**Business**", "**Business Purpose**", "**Consumer**", "**California Consumer**", "**Service Provider**" and "**Sell**" shall have the meaning ascribed to them in the CCPA. "**Data Subject**" shall also mean and refer to "**Consumer**" as such term is defined in the CCPA. "**Personal Data**" shall also mean "**Personal Information**" for the purpose of this DPA.

1.4 "**Customer Data**" means any and all Personal Data, Special Categories of Personal Data or Protected Health Information uploaded by the Customer to the Platform and processed on behalf of the Customer by NovaSight for the purpose of performing the services.

1.5 "**Data Protection Laws"** means any and all applicable privacy and data protection laws and regulations (including, where applicable, EU Data Protection Law and HIPAA) as may be amended or superseded from time to time.

1.6 **"EU Data Protection Law"** means the (i) EU General Data Protection Regulation (Regulation 2016/679) ("**GDPR**"); (ii) Regulation 2018/1725; (iii) any national data protection laws made under, pursuant to, replacing or succeeding (i) and (ii); and (iv)any legislation replacing or updating any of the foregoing.

1.7 "**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996 as amended by the Health Information Technology for Economic and Clinical Health Act (Title XIII of the American Recovery and Reinvestment Act of 2009), and their implementing rules and regulations codified at 45 C.F.R. Parts 160 and 164, each as may be amended from time to time.

1.8 "**Regulatory Authority**" means any national or state (in the case of the United States), or local authority of any government of any country having jurisdiction over the performance of this DPA (including any governmental division, prefecture, subdivision, department, agency, bureau, branch, office, commission, council, court or other tribunal).

1.9 "**Security Incident"** means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data, Special Categories of Personal Data or Protected Health Information of the other party or that has been collected by the other party. For the avoidance of doubt, any Personal Data Breach of the other party's Personal Data, Special Categories of Personal Data or Protected Health Information, will comprise a Security Incident.

1.10 "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council adopted by the European Commission Decision 2021/914 of 4 June 2021.

2. RELATIONSHIP OF THE PARTIES

2.1 The parties acknowledge that in relation to all Customer Data, as between the parties, Customer is the **Controller** of Customer Data, and that NovaSight, in providing the services is acting as a **Processor** on behalf of the Customer. Without derogating from the above, it is hereby clarified that in addition to NovaSight's capacity as a Processor of the Customer Data, NovaSight is also a Controller of certain Personal Data related to the Customer, such as (without limitation) Customer's registration data, Customer's personnel contact details or the Customer's contact information in the event the Customer contacts NovaSight via email. Such Personal Data shall be used and processed in accordance with NovaSight's Privacy Policy.

2.2 The purpose, subject matter and duration of the Processing carried out by NovaSight on behalf of the Company, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects are described in **ANNEX I** attached hereto.

3. REPRESENTATIONS AND WARRANTIES

3.1 The Customer represents and warrants that its Processing activities of Customer Data is in compliance with Data Protection Laws, including by establishing a lawful basis if and as required, and that the instructions provided to NovaSight shall comply with applicable Data Protection Law. In the event EU Data Protection or CCPA do not apply to the Customer, then Customer must abide by whatever other Data Protection Laws and data security laws and regulations applicable to it, and at a minimum: **(i)** obtain and maintain any and all authorizations, permissions and informed consents, as may be necessary under applicable laws and regulations, in order to allow NovaSight to lawfully process and use the Customer Data within the scope of the services; and **(ii)** have, properly publish and abide by an appropriate privacy policy that complies with all applicable Data Protection Laws.

3.2 NovaSight represents and warrants that: **(i)** it shall process the Customer Data on behalf of the Customer, solely for the purpose of providing the services and for the pursuit of a Business Purpose as set forth under the CCPA, all in accordance with Customer's written instructions including as set forth in the Agreement and this DPA; and **(ii)** in the event NovaSight is required under applicable laws to Process Customer Data other than as instructed by Customer, NovaSight shall make its best efforts to inform the Customer of such requirement prior to Processing such Customer Data, unless prohibited under applicable law.

3.3 NovaSight shall take reasonable steps to ensure **(i)** the reliability of its staff and any other person acting under its supervision who may come into contact with or otherwise have access to and Process the Customer Data; **(ii)** that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and **(iii)** ensure that such personnel is aware of their responsibilities under this DPA and any Data Protection Laws.

4. PROCESSING OF PERSONAL DATA AND COMPLIANCE WITH DATA PROTECTION LAW

NovaSight shall be permitted to use and/or disclose Customer Data for the following purposes: (i) provide the service and maintain support of the Platform; (ii) internal purposes; (iii) maintaining and producing Patient Account records, providing monthly detailed reports of accounting by Patient revenue codes, including identifying all co-insurance and deductibles outstanding and including copies of all remittance advice and forms as NovaSight may require for the performance of the services; (iv) for stated purposes permitted under HIPAA; (v) for proper management and administration purposes or to carry out its legal responsibilities, provided however that: (a) such disclosure is required by law; or (b) that NovaSight obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, that such person shall use appropriate safeguards to prevent use or disclosure of the information, and the person immediately notifies NovaSight of any instance of which the confidentiality of the information has been breached; or (v) to provide data aggregation services as defined under HIPAA relating to the health care operations of the Customer.

5. DATA SUBJECT RIGHTS

It is agreed that where NovaSight receives a request from a Data Subject or an applicable authority in respect of Customer Data Processed by it, where relevant, NovaSight will direct the Data Subject or the applicable authority to the Customer in order to enable the Customer to respond directly to the Data Subject's or the applicable authority's request, unless otherwise required under applicable laws. Both parties shall provide each other with commercially reasonable cooperation and assistance in relation to the handling of a Data Subject's or applicable authority's request, to the extent permitted under Data Protection Laws.

6. SUB-PROCESSOR

6.1 The Customer acknowledges that NovaSight may transfer Customer Data to and otherwise interact with third party data processors ("**Sub-Processor**"). The Customer hereby, authorizes NovaSight to engage and appoint such Sub-Processors to Process Customer Data, as well as permits each Sub-Processor to appoint a Sub-Processor on its behalf. NovaSight may continue to use those Sub-Processors already engaged by it, as listed in **ANNEX III,** and NovaSight may engage an additional or replace an existing Sub-Processor to Process Customer Data provided that it notifies the Customer of its intention to do so.

6.2 NovaSight will, where it engages any Sub-Processor, impose, through a legally binding contract between NovaSight and the Sub-Processor, data protection obligations no less onerous than those set out in this DPA on the Sub-Processor. NovaSight shall ensure that such contract will require the Sub-Processor to provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the Data Protection Laws.

6.3 NovaSight shall remain fully responsible for the performance of the Sub-Processors obligations, and shall notify the Customer of any failure by the Sub-Processor to fulfill its contractual obligations.

7. TECHNICAL AND ORGANIZATIONAL MEASURES

7.1 Taking into account 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, without prejudice to any other security standards agreed upon by the parties, NovaSight shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and in accordance with best industry practices to protect data from a Security Incident. Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures.

7.2 Technical and organizational measures implemented by NovaSight to ensure an appropriate level of security are further detailed in **ANNEX II**.

8. SECURITY INCIDENT

NovaSight will notify the Customer upon becoming aware of any confirmed Security Incident involving the Customer Data in NovaSight's possession or control, as determined by NovaSight in its sole discretion. NovaSight's notification regarding or response to a Security Incident under this Section shall not be construed as an acknowledgment by the Company of any fault or liability with respect to the Security Incident. NovaSight will, in connection with any Security Incident affecting the Customer Data: (i) quickly and without delay, take such steps as are necessary to contain, remediate, minimize any effects of and investigate any Security Incident and to identify its cause; (ii) co-operate with the Customer and provide the Customer with such assistance and information as it may reasonably require in connection with the containment, investigation, remediation or mitigation of the Security Incident; (iii) notify the Customer in writing of any request, inspection, audit or investigation by a Regulatory Authority or other authority or litigation arising out of or related to such Security Incident and provide full cooperation to the Customer in responding to such event; and (iv) update the Customer as necessary and provide sufficient information to allow the Customer to meet legal and contractual obligations, including pertaining to any proposed notification to a Regulatory Authority and/or Data Subject.

9. AUDIT RIGHTS

9.1 NovaSight shall respond to inquiries from the Customer regarding the Processing of Personal Data in accordance with this DPA, and shall further make available to the Customer all information necessary to demonstrate compliance with the obligations under the EU Data Protection Laws.

9.2 NovaSight shall make available, solely upon prior written notice and no more than once per year, to a reputable auditor nominated by the Customer, any and all information necessary to reasonably demonstrate compliance with this DPA and applicable Data Protection Laws, and shall allow audits, including inspections, by such reputable auditor solely in relation to the Processing of the Customer Data ("**Audit**") in accordance with the terms and conditions hereunder. The Audit shall be subject to the terms of this DPA and confidentiality obligations (including towards third parties). NovaSight may object in writing to an auditor appointed by the Customer in the event that NovaSight reasonably believes that the auditor is not suitably qualified or independent, a competitor of NovaSight or otherwise unsuitable ("**Objection Notice**"). The Customer will appoint a different auditor or conduct the Audit itself upon its receipt of an Objection Notice from NovaSight. The

Customer shall bear all expenses related to the Audit and shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to NovaSight's premises, equipment, personnel and business while its personnel are on those premises during such Audit. Any and all conclusions of such Audit shall be confidential and reported back to NovaSight immediately. Notwithstanding the aforementioned, NovaSight shall make Personal Health Information available as required to provide an accounting of disclosures in accordance with HIPAA.

10. DATA TRANSFER

10.1 The Customer acknowledges and agrees that in order to provide the services NovaSight might transfer (or access) Customer Data from countries outside the EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) (collectively, "**EEA**"), Switzerland and the United Kingdom ("**UK**"), or an Adequate Country (as such transfers to permitted countries do not require Standard Contractual Clauses or an alternative transfer mechanism), as detailed herein.

10.2 In the event the Processing includes transferring of Personal Data from the EEA, Switzerland or the UK to other countries and such transfers are not performed through an alternative recognized compliance mechanism as may be adopted by NovaSight for the lawful transfer of processing Personal Data outside the EEA, Switzerland or the UK, as applicable or is not exempt under Article 49 of the GDPR (collectively "**Restricted Transfer**"), the following shall apply:

10.2.1 In order to maintain the integrity, security and confidentiality of the Personal Data, a Restricted Transfer shall be subject, in addition to the terms of this DPA, to the terms and obligations of the **Module II** of the Standard Contractual Clauses in which NovaSight shall be deemed as the Data Importer and the Customer shall be deemed as the Data Exporter.

10.2.2 The purpose and description of the transfer shall be detailed in **ANNEX I**.

10.3 The Customer further agrees that where NovaSight engages a Sub-Processor, and those processing activities include a Restricted Transfer, NovaSight and the Sub-Processor shall be bound by the Standard Contractual Clauses in which NovaSight shall be deemed as the Data Exporter and the Sub-Processor shall be deemed as the Data Importer. For the purposes of such engagement, NovaSight and the Sub-Processor will enter into **Module III** of the Standard Contractual Clauses.

10.4 Subject to Clause 13 of Standard Contractual Clauses, NovaSight agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Standard Contractual Clauses.

10.5 Measures and assurances regarding U.S. government surveillance ("**Additional Safeguards**") are further detailed in **ANNEX II**.

11. TERM & TERMINATION

11.1 This DPA shall be effective as of the date the Customer completes the registration process for the services, in accordance with the Agreement and shall remain in force until the services are terminated.

11.2 Following termination of this DPA, NovaSight shall, at the choice of the Customer, delete the Customer Data processed on behalf of the Customer and certify to the Customer that it has done so, or return all the Customer Data to the Customer and delete existing copies unless applicable law or regulatory requires the storage of the Customer Data. Until the data is deleted or returned, NovaSight shall continue to ensure compliance with this DPA.

12. CONFLICT

In the event of a conflict between the terms and conditions of this DPA and the Agreement, this DPA shall prevail. Except as set forth herein all of the terms and conditions of the Agreement shall remain in full force and effect.

ANNEX I

DETAILS OF PROCESSING AND TRANSFERRING OF CUSTOMER PERSONAL DATA

This **ANNEX I** includes certain details of the Processing of Customer Data as required by Article 28(3) GDPR and details of transferring Personal Data subject to the Standard Contractual Clauses.

Categories of data subjects whose personal data is processed or transferred:

- Patients
- Legal Guardian

Categories of personal data processed and transferred:

- Customer Data which shall include Personal Data and Special Categories of Personal Data of the Customer's Patients which may include the following:
  - The Patient's full name
  - ID number
  - Date of birth
  - Gender
  - Last visit to the site where the Patient is being seen; and
  - Certain health information of the Patient including test results.
- Legal Guardian contact details

Sensitive data processed or transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measure:

NA

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Continuous basis.

Nature of Purpose(s) for the processing and transferring on behalf of the controller:

To provide the Services.

Duration of the processing:

The duration shall be for the duration of the Term or until the Customer requests its deletion.

For transfers to (sub-) Processors, also specify subject matter, nature and duration of the processing.
The sub-processors are hosting services and support services, all of the above is applicable to the sub-processors.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES

NovaSight is committed to provide transparency regarding the security measures implemented in order to secure and protect Personal Data processed by the Company for the purpose of providing its services.

The security objectives of the Company are identified and managed to maintain a high level of security and consists of the following (concerning all data assets):

- **Availability** - information and associated assets should be accessible to authorized users when required. The computer network must be resilient. The Company must detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems, and information.
- **Confidentiality** - ensuring that information is only accessible to those authorized to access it, on a need-to-know-basis.
- **Integrity** - safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorized modification, of electronic data.

The purpose of NovaSight information security management system is to:

- Protect and ensure the availability, confidentiality, and integrity of the Company systems, the Customer's, Patient's and Legal Guardian's data, and other Company information systems.
- Enable advanced computing services to support the business processes and the Company goals.
- Detect, prevent, and respond with the best measures to cyber-attack or other information security incidents that may have impact on the company assets.

The following policies are maintained by the Company in order to ensure the measures set forth above. The policies are updated on an ongoing basis and reviewed annually for gaps:

- Data protection procedure
- Privacy Policy Procedure
- Data breach notification procedure
- Data subject access request under the GDPR
- Cyber security Risk Management Procedure
- Cyber security PMS management Procedure
- Software Life Cycle Procedure

As part of our data protection compliance process, we have implemented technical, physical and administrative security measures to protect the Personal Data and/or Personal Information (used herein as "Personal Data" collectively") as explained below.

Physical Access Control

The Company ensures the protection of the data servers which store the Personal Data for the Company from unwanted physical access. The data processed by the Company is stored in the AWS cloud and the Dropbox data servers. The Company also secures physical access to its offices by ensuring that only authorized individuals such as employees and authorized external parties (maintenance staff, visitors, etc.) can access the Company's offices by using security locks and an alarm system, amongst other measures as well.

System Control

Access to the Company's database is highly restricted in order to ensure that only relevant personnel who have received prior approval can access the database. The Company has also implemented appropriate safeguards related to remote access and wireless computing capabilities. Employees are assigned private passwords that allow strict access or use to Personal Data, all in accordance with such employee's position, and solely to the extent such access or use is required. There is constant monitoring of access to the Personal Data and the passwords used to gain access. In addition to password login, two-factor authentication ("**2FA**") provides an added layer of security to Company's database. The Company is using automated tools to identify non-human login to minimize the risk of a brute force attack.

Data Access Control

User authentication measures have been put in place in order to ensure that access to Personal Data is restricted solely to those employees who have been given permission to access it and to ensure that the Personal Data is not accessed, modified or deleted without specific authorization for such actions to be done. Any access to Personal Data, as well as any action performed involving the use of Personal Data requires a password and username, which is routinely changed, as well as blocked when applicable. Each employee is able to perform actions solely in accordance with the permissions granted to him by the Company. Furthermore, the Company conducts ongoing reviews of the employees who have been given authorization to access Personal Data, in order to assess whether such access is still required. The Company revokes access to Personal Data immediately upon termination of employment.

Log Management

NovaSight has implemented a central read-only log repository which provides search All actions in the NovaSight systems are. NovaSight does not allow customers to access logs. However, in case of a court order or official investigation, NovaSight will provide the required information.

Organizational and Operational Security

The Company puts a lot of effort and invests a lot of resources into ensuring that the Company's security policies and practices are being complied with, including by continuously providing employees with training with respect to such security policies and practices. The Company strives to raise awareness regarding the risks involved in the processing of Personal Data. In addition, the Company has implemented applicable safeguards for its hardware and software, including by installing firewalls and anti-virus software on applicable Company hardware and software, in order to protect against malicious software.

Transfer Control

All transfers of Personal Data are protected by the use of encryption safeguards The Company's servers are protected by industry best standards. In addition, to the extent applicable, the Company's business partners execute an applicable Data Processing Agreement, all in accordance with applicable laws. The Company conducted a transfer impact assessment ("**TIA**") identifying all transfers of Personal Data and is able to share the TIA upon Customer's request. The purpose of transfer control is to ensure that Personal Data cannot be read, copied, modified or removed by unauthorized parties during the electronic transmission of these data or during their transport or storage in the applicable data center. Further, any and all transfers of the data (either between the servers, from client side to server side and between Company's designated partners) is secured (HTTPS). Default encryption is implemented in transit and rest.

Availability Control

Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident were implemented by the Company and include an automated backup procedure. The Company has a backup concept which includes automated daily backups. The Company has also implemented Business Continuity plans and Disaster Recovery policies so that in the event of a disaster the Company will be able to continue to provide the services.

Data Retention

Personal Data is retained for as long as needed for us to provide our services or as required under applicable laws.

Job Control

All of the Company's employees are required to execute an employment agreement which includes confidentiality provisions as well as applicable provisions binding them to comply with applicable data security practices. In the event of a breach of an employee's obligation or non-compliance with the Company's policies, the Company implements certain repercussions in order to ensure compliance with the Company's policies. In addition, prior to the Company's engagement with third party contractors, the Company undertakes diligence reviews of such third-party contractors. The Company agrees with third party contractors on effective rights of control with respect to any Personal Data processed on behalf of the Company. The Company ensures that it enters into data protection agreements with all of its clients and service providers.

Software Development Life Cycle

Software development and change management at NovaSight are performed in a manner to help ensure applications are properly designed, tested, approved and aligned to NovaSight's Customers' business objectives. Changes are discussed, evaluated and approved by relevant managers from product, development and operations. Personnel responsibilities for the design, acquisition, implementation, configuration, modification, and management of systems are assigned. In addition, changes performed to the application are communicated to NovaSight's Customers through release notes published on the NovaSight customer success website.

Contractual Obligations

Company has ensured all documents, including without limitations, agreements, privacy policies online terms, etc. are compliant with the Data Protection Regulations, including by implementing Data Processing Agreement and where needed Standard Contractual Clauses (either pursuant to the GDPR and adopted by the European Commission **Decision 2021/914** of 4 June 2021 which is attached herein by linked reference: https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN or pursuant to the standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR for transferring Personal Data outside of the EEA or UK).

Additional Safeguard

Measures and assurances regarding U.S. government surveillance ("**Additional Safeguards**") have been implemented due to the EU Court of Justice Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems decision ("**Schrems II**"), these measures include the following:

- Encryption both in transit and at rest;
- As of the date of this DPA, Sentry has not received any national security orders of the type described in Paragraphs 150-202 of the Schrems II decision.
- No court has found NovaSight to be the type of entity eligible to receive process issued under FISA Section 702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C § 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition.
- NovaSight shall not comply with any request under FISA for bulk surveillance, i.e., a surveillance demand whereby a targeted account identifier is not identified via a specific "targeted selector" (an identifier that is unique to the targeted endpoint of communications subject to the surveillance).
- NovaSight shall use all available legal mechanisms to challenge any demands for data access through national security process that Sentry receives, as well as any non-disclosure provisions attached thereto.
- NovaSight will notify Customer if NovaSight can no longer comply with the Standard Contractual Clauses or these Additional Safeguards, without being required to identify the specific provision with which it can no longer comply.

Penetration Testing

External penetration test is performed after significant change in the system software. The penetration tests include, among others, procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own. The penetration tests and security scans are performed by a reputable Third-party vendor. In addition, NovaSight conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations after significant change in the system software or environment. Actions are taken to remediate identified deficiencies on a timely basis. Vulnerability scans is performed using external tools, in order to detect potential security breaches

Reporting a Security Issue

NovaSight is exerting considerable resources to ensure a secure code and infrastructure for all of its products. If you believe that you have found a security vulnerability in any of our products, please report it to us straight away via e-mail privacy@nova-sight.com Please be sure to include a brief description, detailed steps to reproduce and what might be the impact.

Responsible Disclosure Policy

We encourage responsible disclosure, and we promise to investigate all legitimate reports and fix any issues as soon as we can. We ask that during your research you make every effort to maintain the integrity of our any data you come across, avoiding violating the privacy of any person or degrading our offerings. Please provide NovaSight reasonable time to fix any vulnerability you find before you make it public. In return we promise to investigate reports promptly and not to take any legal action against you.

ANNEX III

SUB-PROCESSORS LIST

Table 1: Sub-Processors List

Processor	Server Location	Service
Eyecare Provider (ECP)	Frankfurt, Germany	Create patient and monitoring treatment
Independent Diagnostic Testing Facility (IDTF)	Frankfurt, Germany	Support

EXHIBIT B

BUSINESS ASSOCIATE ADDENDUM

This Business Associate Addendum ("**BAA**") is executed between NovaSight Ltd. and the Customer, and reflects the parties' obligations and rights with respect to the processing of Patients' Protected Health Information (as such term is defined under the HIPAA).

1. DEFINITIONS

1.1 For the purposes of this BAA, the following capitalized terms shall have the meanings ascribed to them in the HIPAA Rules: Breach, Business Associate, Designated Record Set, Disclosure, Individual, Minimum Necessary, Notice of Privacy Practices, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use. For the purpose of this BAA "Individual" shall also mean the Patient and/or its Legal Guardian.

1.2 "HIPAA" means the privacy, security, breach notification, and enforcement regulations issued by the United States Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996;

1.3 "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information codified at 45 CFR Part 164, Subparts E.

1.4 "Protected Health Information" or "PHI" means any information, whether oral or recorded in any form or medium that is used by NovaSight, on behalf of the Customer, that identifies the Patient or might reasonably be used to identify the Patient and relates to: (i) its past, present or future physical or mental health; (ii) the provision of health care services to the Patient; (iii) the past, present or future payment for health care services.

1.5 "Security Rule" means the Standards for Protection of Electronic Protected Health Information, codified at 45 CFR Parts 164, Subpart C.

1.6 "Breach Notification Rule" means "Notification in the Case of Breach of Unsecured Protected Health Information" codified at 45 CFR Part 164, Subpart D.

2. CONFIDENTIALITY AND HIPAA

2.1 With respect to the PHI which may be processed during the provision of the services, the parties hereby acknowledge and agree that the Customer is the **Covered Entity** while NovaSight is the **Business Associate** or **Service Provider**.

2.2 NovaSight acknowledges that, as between the Parties, all Personal Data and PHI managed within the System, shall be and remain the sole property of the Customer. It shall be clarified that, this BAA does not address or limit the processing of anonymous or de-identified data which can no longer be identified or associated with a natural person (in accordance with section 164.514(a) of the HIPAA Privacy Rule), even if such anonymized data was produced using PHI;

2.3 The Parties shall comply with all federal and state laws governing the confidentiality and privacy of health information that are applicable to them, respectively, including, without limitation, HIPAA and the HIPAA Rules. The Customer shall have sole responsibility for the accuracy, quality, and legality of PHI fed to the System by the Customer or anyone on its behalf, and the legality of the means by which such PHI was acquired.

3. USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

3.1 NovaSight shall strictly keep the confidentiality of the PHI, and shall use or disclose PHI only in connection with fulfilling its duties and obligations under this BAA and the License Agreement.

3.2 Notwithstanding the above, NovaSight may use PHI received from the Customer in the following events:

3.2.1 For the performance of the services set forth in the License Agreement;

3.2.2 As required by law; or

3.2.3 In a manner that would not violate Subpart E of 45 CFR Part 164 if done by the Customer, except that NovaSight may use PHI to carry out its the legal responsibilities only after obtaining reasonable assurances from the person to whom the information is disclosed to that the information will remain confidential and used or further disclosed only as and to the extant required by law or for the purposes for which it was disclosed to the person, and that person agrees to notify NovaSight of any instances of which it is aware in which the confidentiality of the information has been breached.

4. DATA SECURITY AND SAFEGUARDS

4.1 NovaSight shall use appropriate safeguards and data security measures and comply with Subpart C of 45 C.F.R. Part 164 of HIPAA with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by this BAA.

4.2 NovaSight shall employ appropriate administrative, technical and physical safeguards, consistent with the size and complexity of Subcontractor's operations, comply with applicable requirements of this BAA, the Privacy Rule, the Security Rule and the Breach Notification Rule to protect the confidentiality of PHI and to prevent the use or disclosure of PHI in any manner inconsistent with the terms of this BAA.

4.3 Those measures shall include (as a minimum and in accordance with its relevance):

- Implementation of security-related policies and procedures, standards and practices designated for the protection of PHI;
- Minimalization of PHI processing where possible and reasonable;
- Use of encryption and pseudonymization;
- Implementation of data protection measures by default and by design;
- The use of proper firewalls and antivirus systems;
- Managing organizational passwords policy which enforces complexity requirements;
- Managing strict access authorization policy which ensures that any access to PHI by NovaSight employees shall be strictly limited to employees which are in need for that data, for the provision of the services;
- Keeping backup and recovery capabilities;
- The use of other state of the art technological and organizational controls mitigating data protection risks or any data breach or loss.

5. AVAILABILITY OF BOOKS AND RECORDS

5.1 NovaSight shall permit the Customer and the Secretary to audit NovaSight's internal practices, books and records as they pertain to the use and disclosure of PHI received from, or created or received by NovaSight on behalf of the Customer and at reasonable times, in order to determine its compliance with the HIPAA Rules.

5.2 The parties agree to comply with audit requirements presented by the U.S. Department Health and Human Services' Office for Civil Rights regarding their compliance with applicable laws including the Health Information Technology for Economic and Clinical Health Act ("**HITECH**").

6. ACCESS, AMENDMENT AND ACCOUNTING OF DISCLOSURES

6.1 NovaSight, within ten (10) business days of a written request by the Customer, shall:

6.1.1 Make available to the Customer any PHI contained in a Designated Record Set which is available to NovaSight and was not transferred to the Customer, in accordance with 45 CFR Section 164.524.

6.1.2 Make any amendment(s) to PHI in a Designated Record Set as directed or agreed to by the Customer pursuant to 45 C.F.R. §164.526, or take other measures as necessary to satisfy the Customer's obligations under 45 C.F.R. §164.526.

6.1.3 make available the information required to provide an accounting of disclosures to the Customer as necessary to satisfy the Customer's obligations under 45 C.F.R. §164.528;

6.2 In the event NovaSight receives a request from a Patient or its legal Guardian, in connection with such Patient's PHI (whether a request for access, amendment, accounting of disclosures or any other request of any nature or description), NovaSight shall immediately notify the Customer of such request and cooperate with the Customer instructions in responding to such request.

6.3 NovaSight's assistance may be provided by implementing relevant interfaces in the System, in a manner which provides the Customer with all relevant information and features required for him for addressing any such request or legal obligation;

7. ENGAGING EXTERNAL SUPPLIERS AND SUBCONTRACTORS

NovaSight shall obtain and maintain a written agreement with each Subcontractor and agent of NovaSight which process, receives, maintains, or transmits PHI, pursuant to which agreement such Subcontractor and agent agrees to be bound by the same restrictions, terms, and conditions that apply to NovaSight under this BAA.

8. REPORTING OF BREACHES

8.1 In the event of a Breach of any Unsecured PHI that NovaSight accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds or uses on behalf of the Customer, NovaSight shall report such Breach to the Customer as soon as practicable, but in no event later than 48 hours after the date the Breach is discovered by NovaSight.

8.2 Notice of a Breach shall include, at least: (i) if possible, the identification of each Individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed during the Breach; (ii) the date of the Breach, if known, and the date of discovery of the Breach; (iii) the scope of the Breach, including the results of the risk assessment of whether there is a low probability that the PHI has been compromised based on the required factors set forth in 45 CFR 164.402; (iv) NovaSight's response to the Breach; and (v) any other information the Customer

reasonably requests in order to assess the nature and scope of the breach and accompanying mitigation measures.

8.3 In the event of a Breach, NovaSight shall, in consultation with the Customer, mitigate, to the extent practicable, any harmful effect of such Breach that is known to NovaSight.

9. THE CUSTOMER'S OBLIGATIONS

9.1 The Customer shall notify NovaSight of any limitation(s) in any applicable notice of privacy practices in accordance with 45 CFR Section 164.520 to HIPAA of which it becomes aware, to the extent that such limitation may affect NovaSight's use or disclosure of PHI.

9.2 The Customer shall notify NovaSight of any changes in, or revocation of, permission by Individual to use or disclose PHI of which it becomes aware, to the extent that such changes may affect NovaSight's use or disclosure of PHI.

9.3 The Customer shall notify NovaSight of any restriction to the use or disclosure of PHI that the Customer has agreed to in accordance with 45 CFR Section 164.522 to HIPAA of which it becomes aware, to the extent that such restriction may affect NovaSight's use or disclosure of PHI.

9.4 The Customer shall not request NovaSight to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 CFR Part 164 to HIPAA if done by the Customer.

10. MISCELLANEOUS

10.1 Except as amended by this BAA, the License Agreement shall remain in full force and effect.

10.2 This BAA is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter. In the event of any conflict between the terms of this BAA and the License Agreement, the terms of this BAA shall prevail so far as the subject matter concerns the processing of PHI.

10.3 NovaSight's liability under this BAA is subject to the same limitations on liability contained in the License Agreement.