NovaSight

CureSight™

Amblyopia Treatment System

Model-CS100

Privacy Policy Package

Authorization			
	Name	**Title**	**Signature and Date**
Written By	Hilla Shribman	APM& CO., External Adv.	Hilla Shribman 23-May-23
Reviewed By	Tal Samet	Project Manager	Digitally signed by Tal Samet Date: 2023.05.24 11:16:59 +03'00'
Reviewed By	Liron Rosenbaum	VP Strategy	Digitally signed by Liron Rosenbaum Date: 2023.05.24 18:16:05 +03'00'
Reviewed & Approved By	Margaux Zenou	QA/RA Manager	Digitally signed by Margaux Zenou Date: 2023.05.28 12:09:18 +03'00'
Reviewed & Approved By	Ran Yam	CEO	Digitally signed by Ran Yam, CEO Date: 2023.05.28 12:13:13 +03'00'

Revision History

Rev	Description of change	CAPA/ECO	Written By	Effective Date
01	Initial Release	N/A	Tal Samet	04-Apr-2022
02	General Periodic updates	N/A	APM & Co.	Once signed

Table of Contents

Table of Tables

PRIVACY POLICY

[Last Updated 18th May, 2023]

1. GENERAL

NovaSight Ltd. and NovaSight Inc. (collectively, "**NovaSight**," "**we**," "**our**," or "**us**") is the developer and owner of the CureSight™ digital amblyopia medical device ("**Device**") and web-based cloud platforms for diagnosis and care management ("**Platform**"). The Device is provided and distributed by our partners and used by patients. The Platform is used by healthcare providers and Independent Diagnostic Testing Facilities known ("**IDTF**") (collectively **Eye Care Providers** or "**ECP**").

This Privacy Policy describes how we process information on and from the ECPs, the patients and their legal guardians, as the patients are children (collectively "**you**" or "**your**").

In addition to this Privacy Policy, please review the following:

- **Notice of Privacy Practices (see EXHIBIT B)**: Any information which relates eye care services, identified with an individual who is the subject of such eye care services is considered under the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") as Personal Health Information ("**PHI**"). Therefore, even though we solely provide the technology and are considered the manufacture, which is not a "covered entity" under the HIPAA, we take the confidentiality of PHI very seriously therefore we choose to adopt the strict HIPAA Rules in maintaining the PHI as further detailed in the Notice of Privacy Practices.
- **CCPA Notice (see EXHIBIT A)**: The California Consumer Privacy Act ("**CCPA**") requires a "Business" provides individuals with a notice disclosing the personal information collected and the rights an individual obtains. Colorado, Virginia and Nevada also have similar requirements. If you are a resident of such states, please see the CCPA Notice.
- The ECPs, service providers and care givers might have additional policies or notices concerning the processing of your personal data which we recommend you review.

2. CONTROLLER INFROMATION

As required under the EU and UK General Data Protection Regulations ("**GDPR**") please see the details of the data controller: NovaSight Ltd.

- By email: privacy@nova-sight.com.
- By Telephone: +972-3-642-2868
- By mail: NovaSight Ltd.

  1 Hayarden St. Airport City, Israel 7019801

However, the GDPR, CCPA and HIPAA distinguish between the "controller", "business" and "covered entity", which provide the processing instructions, and the "processor", "service provider". As the manufacture, and operator of the web-based cloud platform, we receive instructions from organization providing you with healthcare services, the ECPs, and usually take the role of the processor.

3. INFORMATION WE COLLECT

(i) **Non-Personal Data:** The first type of data is non-identifiable, anonymous and aggregated data that is mainly technical data transmitted by your device and via your use of the Platform. ("**Non-Personal Data**"). We are not aware of the identity of the individual who we collected the Non-Personal Data from.

(ii) **Personal Data**: The second type of data is individually identifiable information, namely information that identifies an individual or may with reasonable effort identify an individual ("**Personal Data**"). Personal Data includes PHI, if and to the extent applicable.

For the avoidance of doubt, any Non-Personal Data that is linked to any Personal Data.

Below please see the table specifying the data sets collected and the purpose:

Type of Personal Data	Purpose of Processing and Lawful Basis
Registration and Support: When the ECP registers through our Platform, it will provide us with its full name, email address, profession, phone number, and address, medical license, and any additional information required. Additionally, you may provide us with contact information of other care givers or administrators using the Platform for the purpose of proving them with access to the Platform.	This information will be processed for the purpose of performing our contract with you, to set up your account with us and enable you to use our Platform and provide technical or professional support. Further, we will use this information to add you to "Find a Doctor" database.
Usage Data: When you use our Platform, we may, either directly or indirectly (through our third-party service providers) collect your IP address, as well as certain data about your use and interactions with the Platform. This includes technical and usage data transmitted by the computer, click stream data, access logs, errors, and duration of use. Through the Device, we collect the patient's usage data, meaning how many hours did the patient use the device, the device unique ID which is associated with the patient UUID, and access logs.	We use such data to provide our better customer support, and to improve our services as they relate to such support activities. We further process the patient data on behalf of the ECP so that they can monitor the sufficiency of the treatment.
Patient Data processed on behalf of ECP: The ECP will be uploaded the patient's full name, ID number, date of birth, gender, last visit to the site (i.e., clinic), address, certain health information including vision performance and test, patient ID, Device ID, medical history, medications, current or past treatment and diagnostic inferences drawn from such data.	We store this information solely as the data processor on behalf of the controller or covered entities as such terms are defined under applicable laws. If the collection and use of such data requires any consent or authorization, such consent will be obtained by the controller or covered entities.

Type of Personal Data	Purpose of Processing and Lawful Basis
As patients are children the communication and contact information shall be of such patient's legal guardian.	
Payment and Insurance: We may use and disclose your PHI or health insurance information, so that we, or our service provider, or the health care providers can bill and collect payment from the patient, or its insurance company, or a third party that helps us submit bills and collect amounts owed. We may request additional information such as SSN, payment information (bank account or credit cards), identification information.	We process this data solely to enable the service providers to collect payment on our behalf. Such data is not stored or retained by us. NovaSight may solely document the transaction.

Please note that the actual processing operation per each purpose of use and lawful basis detailed in the table above may differ. Such processing operation usually includes a set of operations made by automated means, such as collection, storage, use, disclosure by transmission, erasure, or destruction. The transfer of personal data to third-party countries, as further detailed in the Data Transfer Section, is based on the same lawful basis as stipulated in the table above.

In addition, we may use certain Personal Data to prevent potentially prohibited or illegal activities, fraud, misappropriation, infringements, identity thefts, and any other misuse of the Device or Platform and to enforce the terms, as well as to protect the security or integrity of our databases, and to take precautions against legal liability. Such processing is based on our legitimate interests.

We may collect different categories of Personal Data and Non-Personal Data from you, depending on the nature of your interaction with us. If we combine Personal Data with Non-Personal Data, the combined information will be treated as Personal Data or for as long as it remains combined.

4. HOW WE COLLECT DATA

Depending on the nature of your interaction with us, we may collect information from you in one or both of the following ways:

(i) **Automatically** – we may automatically collect some information from you, such as your IP address, when you use our Platform.

(ii) **Provided by you voluntarily** – we will collect information if and when you choose to provide us with the information, such as via communications with us.

(iii) **Provided by Third Parties**- such as the ECP or service providers.

5. SHARING INFORMATION WITH THIRD PARTIES

We may share your Personal Data with third parties, including our partners or service providers, as detailed in the table below:

CATEGORY OF RECIPIENT	DATA SET	PURPOSE OF SHARING
Service Providers	All types of Personal Data	We share Personal Data with the following service providers: hosting and server co-location services, communications and content delivery networks (CDNs), data and cyber security, package delivery and tracking services, customer support call centers, session, call or activity recording and analysis, remote access, performance measurement, customer management systems, and any other relevant service.
Affiliated companies or acquiring company	All types of Personal Data.	We may share Personal Data, in the event of, or during negotiations of, a corporate transaction (e.g., sale of a substantial part of our business, merger, consolidation or asset sale). In the event of the above, our affiliated companies or acquiring company will assume the rights and obligations as described in this Privacy Policy.
Governmental agencies, or authorized third parties, FDA, agencies, etc.	Subject to applicable law or enforcement authority request.	In exceptional circumstances, we may disclose or allow government and law enforcement officials access to your personal data, in response to a subpoena, search warrant, or court order (or similar requirement), or in compliance with applicable laws and regulations. Such disclosure or access may occur if we believe in good faith that: (a) we are legally compelled to do so; (b) disclosure is appropriate in connection with efforts to investigate, prevent, or take action regarding actual or suspected illegal activity, fraud, or other wrongdoing; or (c) such disclosure is required to protect our legitimate business interests. Further, we may be required to transfer your details to relevant authorities such as the FDA, as part of our legal obligations as a medical device manufacturer. Further, we may use share your Personal Data as part of any regulatory audit we are subjected to.

ECP, healthcare providers and support services	Patient Data	We share and process such data on behalf of your physician or healthcare provider's administrative personnel that may access your data on behalf of your healthcare provider, and will be able to monitor, process, and analyze it. We may also share your personal data directly with third-party service providers engaged by your healthcare provider, or receive certain relevant data from your healthcare provider's behalf on the third-party provider's service.
Third party that helps us submit bills and collect amounts owed.	Any data related to reimbursement claims and payments.	We, directly or through the use of relevant third party providers, and as per your request, will file reimbursement claims on your behalf, to your insurer or in order to collect payment. The aforesaid is usually applicable in the US and not under EU jurisdiction.

In addition, and without derogating from the generality of the above, we may share your information following any separate and independent consent or authorization provided by you to us, anyone on our behalf or any third party.

6. DATA RETENTION

We retain the information we collect as long as it remains necessary for the purposes set forth above, all in accordance with applicable laws.

In some circumstances, we may store your Personal Data for longer periods of time, for instance where we are required to do so in accordance with legal, regulatory, tax, audit, accounting requirements and so that we have an accurate record of your dealings with us in the event of any complaints or challenges, or if we reasonably believe there is a prospect of litigation relating to your Personal Data or dealings. To determine the appropriate retention period, we consider the amount, nature, and sensitivity of the Personal Data, the potential risk of harm from unauthorized use or disclosure of your Personal Data, the purposes for which we process your Personal Data, and whether those purposes can be achieved through other means, as well as applicable legal requirements.

Retention periods of Personal Data processed by us as a Processor, may also be affected by the controllers' instructions.

We may at our sole discretion, delete or amend information from our systems, without providing any notice to you, once we deem it is no longer necessary for our purposes.

7. USER RIGHTS

Depending on your jurisdiction and your interaction with us, data protection and privacy laws provide you with the ability to exercise certain rights regarding your Personal Data that we process or have access to, such as under the GDPR: **(i)** the right to access your Personal Data; **(ii)** the right of rectification; **(iii)** the right to the erasure of your Personal Data; **(iv)** the right to restrict the processing of your Personal Data; **(v)** the right to object to the processing

of your Personal Data; **(vi)** data portability; **(ix)** the right to file a complaint to a supervisory authority **(x)** the right to non-discrimination; and **(xi)** the right to withdraw consent.

If you wish to exercise any or all of the above rights, please send to our privacy team at: privacy@nova-sight.com.

If we are unable to provide you with the information that you asked for, we will endeavor to explain the reasoning for this and inform you of your rights. We reserve the right to ask for reasonable evidence to verify your identity before we provide you with any such information in accordance with applicable law.

Your rights under HIPAA- Please see the Notice of Privacy Practice.

Your rights under the CCPA, or otherwise the Virginia Consumer Data Protection Act ("**VCDPA**"), or Colorado Privacy Act, please see the CCPA Notice.

8. SECURITY

We take great care in implementing and maintaining the security of your information. We employ industry standard procedures and policies to ensure the safety of individuals' information and prevent unauthorized use of any of such.

Please contact us at privacy@nova-sight.com if you believe that your privacy was treated in a way that was not in accordance with this Privacy Policy. In the event of a security incident in which we discover that your Personal Data may be at risk, we will take reasonable efforts to notify you and the applicable authority (if we are required to do so, subject to applicable laws).

9. DATA TRANSFER

We may store or process your Personal Data in the EU, the United States or in other countries. Thus, any information you provide us may be transferred to and processed in countries other than the country from which you access our Platform or use the Device. We will take appropriate measures to ensure that your Personal Data receives an adequate level of data protection upon its transfer. When Personal Data that was collected within the European Economic Area ("**EEA**") is transferred outside the EEA, we will take necessary steps in order to ensure that sufficient safeguards are provided during the transferring of such Personal Data, in accordance with the provision of the Standard Contractual Clauses approved by the European Commission. You may exercise your rights, where applicable, to receive information regarding the transfer mechanism that was used during such transfer.

10. CHANGE TO THIS PRIVACY POLICY

We reserve the right to amend this Privacy Policy at any time. In the event that we made any substantial changes to this Privacy Policy, we will make reasonable efforts to provide you with notification with respect to such changes, if we are required to do so by applicable law. The changes to this Privacy Policy will go into effect as of the date listed in the "Last Amended" heading located at the top of this Privacy Policy.

EXHIBIT A

CCPA NOTICE

[Last Updated: May 17, 2023]

The California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act ("**CPRA**") of 2020 ("**CCPA**"), requires that we, NovaSight Inc., together with its subsidiaries, affiliates, or related companies ("**Company**", "**our**", "**we**" or "**us**") provide California residents (consumers or employees) with notice at collection ("**CCPA Notice**"). The CCPA Notice shall disclose the Personal Information (as defined below) that is collected, processed and shared during the use of the Platform or Device.

This CCPA Notice will also address and apply to Virginia residence and detail additional rights under the Virginia Consumer Data Protection Act ("**VCDPA**") and Colorado residence governed by the Colorado Privacy Act.

The CCPA Notice is an integral part of the Privacy Policy; capitalized terms used but not defined in this CCPA Notice will have the meanings set out in therein or as defined under the CCPA, VCDPA or CPA, as applicable. If there is any conflict or inconsistency between the terms of this CCPA Notice and the Privacy Policy, the terms of this CCPA Notice will prevail solely for eligible consumers.

Part I: A Comprehensive Description of the Information Practices

(A) Categories of Personal Information We Collect

We collect Personal Information which is defined under the CCPA as any information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer, household or device, all as detailed in the table below.

Personal Information under the CCPA includes Sensitive Personal Information ("**SPI**") as detailed in the table below.

Personal Information does **not** include: Publicly available information that is lawfully made available from government records, that a consumer has otherwise made available to the public; de-identified or aggregated consumer information; Information excluded from the CCPA or CPRA scope, such as: Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPPA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data; Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA) and the Driver's Privacy Protection Act of 1994.

We have collected as a "Business" the following categories of Personal Information within the last twelve (12) months:

Category	Example	Collected
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	Yes
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	Yes
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	No
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	No
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	No
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	No
G. Geolocation data.	Physical location, approximate location derived from IP address or movements.	No

H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	No
I. Professional or employment-related information.	Current or past job history or performance evaluations.	No
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	No
K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	No
L. Sensitive personal information.	Social security, driver's license, state identification card, passport number, account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account, precise geolocation, racial or ethnic origin, religious or philosophical beliefs, or union membership, the contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication, genetic data, biometric data, information concerning health, sexual life or sexual orientation.	No

(B) <u>Categories of Sources of Personal Information</u>

Depending on the nature of your interaction with NovaSight, NovaSight collects the Personal Information as follows:

- Automatically collected by us or our service providers.
- Provided by you directly when you reach out.
- Provided by physicians and ECPs.
- Provided by third parties – such as third parties payment providers, insurance companies, etc.

(C) Use of Personal Information

We may use the Personal Information collected as identified above, for the following purposes:

- To fulfill or meet the reason you provided the Personal Information (create your Account);
- To provide the services;
- Respond to law enforcement; or otherwise as detailed in our Privacy Policy.

We will not collect additional categories of Personal Information or use the Personal Information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

(D) Disclosures of Personal Information for a Business Purpose

We may disclose your Personal Information to a contractor or service provider for a business purpose. When we disclose Personal Information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that Personal Information confidential and not use it for any purpose except performing the contract. We further restrict the contractor and service provider from selling or sharing your Personal Information.

In the preceding twelve (12) months, we have disclosed the following categories of Personal Information for a business purpose:

Business Purpose	**Category (corresponding with the table above)**	**Category of Recipient**
Helping to ensure security and integrity to the extent the use of Personal Information is reasonably necessary and proportionate for these purposes.	Category A Category B	Security prevention providers, operating systems.
Debugging to identify and repair errors that impair existing intended functionality		
Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.		Payment processors, IDTF (e.g., customer support), affiliated companies, operating systems, CRM, ERP, health care providers, health insurance, cloud computing and storage vendors, etc.
Undertaking internal research for technological development and demonstration.		Developers, operating systems, cloud and hosting providers.
Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, or controlled by the business, and to improve, upgrade, or		

enhance the service or device that is owned or controlled by the business.		

(E) Sale or Share of Personal Information

In the preceding twelve (12) months, we did not "sell" or "share" any Personal Information.

(F) Children Under the Age of 16

As elaborated above, and under the Privacy Policy, we do collect Personal information from children under the age of 16, subject to such Patients' Legal Guardian's consent.

(G) Data Retention

In general, we retain the Personal Information we collect for as long as it remains necessary for the purposes set forth above, all under the applicable regulation, or until you express your preference to opt-out, where applicable.

The retention periods are determined according to the following criteria:

1. For as long as it remains necessary in order to achieve the purpose for which the Personal Information was initially processed. For example: Account's credentials will be retained for as long as you use the Services.
2. To comply with our regulatory obligations, including for long periods as part of our legal obligations as medical device manufacturer.
3. To resolve a claim, we might have or a dispute with you, including any legal proceeding between us, until such dispute will be resolved, and following, if we find it necessary, in accordance with applicable statutory limitation periods.

Please note that except as required by applicable law, we will not be obligated to retain Personal Information for any particular period, and we may delete it for any reason and at any time, without providing you with prior notice if our intention to do so.

Part II: Your Rights Under the Data Protection Laws

(A) Your Rights

If you are a California, Virginia, Colorado or Nevada residents, you may exercise certain privacy rights related to your Personal Information. You may exercise these rights free of charge except as otherwise permitted under applicable law. We may limit our response to your exercise of these privacy rights as permitted under applicable law, all as detailed herein:

Rights	Details
The right to know what Personal Information NovaSight has collected about you.	Including the categories of Personal Information, the categories of sources from which the Personal Information is collected, the business or commercial purpose for collecting Personal Information, the categories of third parties to whom NovaSight discloses Personal Information, and the specific pieces of Personal Information that NovaSight has collected about you.
Deletion Rights.	The right to delete Personal Information that NovaSight has collected from you, subject to certain exceptions. We reserve the right to reject such request under certain circumstances, and will inform you of the basis for the denial, which may include, but is not limited to, ensure the security and integrity, provide the services, a legal obligation, etc.

Correct Inaccurate Information	The right to correct inaccurate Personal Information that NovaSight maintains about you.
Non-Discrimination	The right not to receive discriminatory treatment by NovaSight for the exercise of privacy rights conferred by the CCPA, including denying a consumer services, charging different prices or rates for services, providing you a different level or quality of services, etc.
Data Portability	You may request to receive a copy of your Personal Information, including specific pieces of Personal Information, including, where applicable, to obtain a copy of the Personal Information you provided to us in a portable format.

Note: You may only exercise this right, unless legally required otherwise, **twice within 12 years**.

(B) How Can You Exercise Your Rights?

You may exercise your rights free of charge except as otherwise permitted under applicable law. We may limit our response to your exercise of these privacy rights as permitted under applicable law, all as detailed herein and by approaching us through the means of contact herein or through our website.

(C) Authorized Agents

You can designate an authorized agent to submit requests on your behalf. However, we will require written proof of the agent's permission to do so and verify your identity directly.

(D) Response Timing and Format

We endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require additional time (up to an additional forty-five (45) days), we will inform you of the reason and extension period in writing by mail or electronically, at your option. If we determine that the request warrants a fee, we will tell you why we made such decision and provide you with a cost estimate before completing your request.

For Virginia Residence: If you have an account with us, we may require you to use the account to submit the VCDPA request. We may require specific information from you to help us confirm your identity and process your VCDPA request. If we denied a request, you may appeal our decision, and within 60 days of our receipt of your appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, you may submit a complaint to the Virginia Attorney General at https://www.oag.state.va.us/consumercomplaintform.

Part III: Other State Laws and Rights

Notice to Virginia Residents: The VCDPA provides Virginia residents with the right to receive certain disclosures regarding the Personal Information we process about them. This CCPA Notice provided any and all needed disclosures under the VCDPA. If you are a Virginia resident, the VCDPA grants you the right to: (1) confirm whether or not we are processing your Personal Information and access such Personal Information; (2) correct inaccuracies in your Personal Information, taking into account the nature of the Personal Information and the purposes of the processing of your Personal Information; (3) delete Personal Information you have provided or we have obtained about you; and (4) obtain a copy of your Personal Information that you previously provided to us in a portable and, to the extent technically

feasible, readily usable format that allows you to transmit the data to another controller without hindrance, where the processing is carried out by automated means. The rights and how to exercise them are detailed under this CCPA Notice and are applicable for Virginia residence as well and you may exercise your rights as detailed above.

Notice to Nevada Residents: Nevada law allows Nevada residents to opt out of the sale of certain types of personal information. Subject to several exceptions, Nevada law defines "sale" to mean the exchange of certain types of personal information for monetary consideration to another person. We currently do not sell personal information as defined in the Nevada law. However, if you are a Nevada resident, you still may submit a verified request to opt out of sales and will record your instructions and incorporate them in the future if our policy changes. You may send opt-out requests to privacy@nova-sight.com.

CONTACT US:

By email: privacy@nova-sight.com

By mail: NovaSight Ltd. 1 Hayarden St. Airport City, Israel 7019801

UPDATES:

This notice was last updated on May 09, 2023. As required under the CCPA, we will update this CCPA Notice **every 12 months**. The last revision date will be reflected in the "Last Updated" heading at the top of this CCPA Notice.

EXHIBIT B-
NOTICE OF PRIVACY PRACTICES
[Last Updated: May 18, 2023]

Securing your Personal Information is our priority, this Notice of Privacy Practice ("**Notice**") is in addition to, and does not replace, the Privacy Policy. Defined terms herein shall have the same meaning as defined in the Privacy Policy.

This Notice describes how we, NovaSight Inc. or NovaSight Ltd., together with its subsidiaries, affiliates, or related companies, the "**Company**", "**our**", "**we**" or "**us**"), may use or disclose certain medical information about you, and how you can get access to this information. Any information which relates to prescription, or the provision of eye care services, identified with an individual who is the subject of such eye care services and considered under the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") as Personal Health Information ("**PHI**"). Therefore, even though we are solely the manufacture of the CureSight medical devise, and the operator of the supporting web-based cloud platform, which are not considered a "covered entity" under HIPAA, however, we take the confidentiality of your PHI very seriously therefore we choose to adopt the strict HIPAA Rules in maintaining the PHI as further detailed below in this Notice.

NovaSight utilizes a secure HIPAA compliance format for encrypting and sending data files. The users are obligated as well to ensure that transfer of any patient records and/or results is performed in accordance with applicable law and ensuring patient confidentiality.

1) USES AND DISCLOSURES OF PHI THAT DO NOT REQUIRE AUTHORIZATION

a) **Treatment**: We may use and disclose your PHI for treatment purposes, we may share the PHI with doctors, eye-care providers, IDTF, and other personnel involved in your health care.
b) **Diagnostic**: The care giver may share your medical history, vision diagnostic, and prescriptions provided by a doctor or optometrist.
c) **Payment**: We may use and disclose your PHI so that we, or our service provider, or the health care providers can bill and collect payment from you, your insurance company, or a third party that help us submit bills and collect amounts owed.
d) **Family Members**: We may disclose your PHI to a family member, other relative, friend, or other individual identified by you, who is involved in your medical care or payment for your care, provided you agree to this disclosure, you had an opportunity to object and did not do so, or we infer from the circumstances in our professional judgment that the disclosure is appropriate.
e) **As Required by Law:** We will disclose your PHI when required to do so by federal, state, or local law.
f) **Safety, Quality Management, Public Health, and FDA**: We may disclose your PHI to relevant authorities to prevent or control product recalls, repairs, or replacements.
g) **Health Oversight Activities**: We may disclose your PHI for legally authorized oversight activities, such as audits, investigations, inspections, and credentialing.

2) USES AND DISCLOSURES OF PHI THAT REQUIRE YOUR AUTHORIZATION

h) **To Communicate with You about Health-Related Products and Services**: We do not communicate with you, however our service providers may use or disclose your PHI to communicate with you regarding your care and related matters. For example,

they may use your PHI to provide reminders, reminders to use the Device or to understand why and how it is used. These communications are done through email or through the CureSight center. You may withdraw your consent and opt-out of these communications at any time.

i) **Marketing**: With your authorization, the PHI may be used PHI for marketing purposes.

3) YOU HAVE THE FOLLOWING RIGHTS CONCERNING YOUR PHI

a. **Access PHI and Receive a Copy**: You have the right to review or get copies of your PHI and health related information, with limited exceptions. You may request that we provide copies in a format other than photocopies. We will use the format you request unless we cannot practicably do so. Please make such request in writing. You may obtain a form to request access by using the contact information listed at the end of this Notice. We may charge you a reasonable cost-based fee for expenses such as copies and staff time. If you request an alternative format, provided that it is practicable for us to produce the information in such format, we may charge a cost-based fee for preparing and transmitting your health information in that format. You have the right to request a copy of your information in electronic format, and to direct us to transmit a copy of your information to a third party designated by you; and our fee may not exceed our labor costs in responding to such request.

b. **Restrict Uses and Disclosures of PHI**: You have the right to request additional restrictions on our use or disclosure of your PHI. We are not required to agree to these additional restrictions. Upon your request, and except as otherwise required by law, we will not disclose your health information to a health plan for purposes of payment or health care operations when the information relates solely to a service or product for which you paid out-of-pocket in full.

c. **Amendment of PHI**: If you feel that PHI we maintain about you is incomplete or incorrect, you may request that we amend it. Your request must be in writing, and it must explain why the information should be amended. We may deny your request under certain circumstances. You may obtain a form to request an amendment to your health information by using the contact information listed at the end of this Notice.

d. **Accounting of Disclosures of PHI**: You have the right to receive a list of instances in which we disclosed your PHI for purposes other than treatment, payment, health care operations, where you have provided an authorization and certain other activities, for the last 6 years (or a shorter period if our relationship with you has existed for less than 6 years). If you request this accounting more than once in a 12-month period, we may charge you a reasonable, cost-based fee for responding to these additional requests.

e. **Notification of a Breach related to PHI**: If we become aware that your PHI has been breached and the privacy or security of the information has been compromised, you have the right to be notified of the breach without unreasonable delay and in no event later than 60 days following our discovery of the breach.

For exercising any rights or requests related to your PHI, please contact the CureSight Monitoring Center at: 888-404-7417 / Novasight@notalvision.com, or NovaSight directly at: privacy@nova-sight.com

4) COMPLAINTS AND CONTACT US

If you have questions or would like further information about this Notice or if you feel we have violated your rights, you may file a complaint by contacting us at privacy@nova-sight.com.

You can also file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting www.hhs.gov/ocr/privacy/hipaa/complaints/. A complaint must be made in writing and will not in any way affect the quality of care we provide you with.

5) CHANGES TO THIS NOTICE

We reserve the right to change this Notice and to make the revised Notice effective for PHI we already maintain or receive in the future. We will post a copy of the current Notice here.