HIPAA PRIVACY POLICY FOR OPTICAL LABS

TABLE OF CONTENTS

HIPAA PRIVACY POLICY FOR OPTICAL LABS

A. INTRODUCTION

This Privacy Policy of *(replace this with your company name)* (the "Lab") is implemented by the Lab for the purpose of complying with the Standards for the Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164 ("Privacy Rule"). In particular, this policy documents how the Lab will treat Protected Health Information (as defined below) in compliance with HIPAA Privacy Regulations, and will otherwise comply with such regulations. This policy applies to all business locations operated by the Lab. A copy of the HIPAA Privacy Regulations is attached hereto at Exhibit A.

B. PRIVACY OFFICIAL

The Privacy Official designated by the Lab as the person responsible for development and implementation of the Lab's HIPAA Privacy Policies and Procedures is (*replace this with the name or title of designated Privacy Official*).

C. CONTACT PERSON OR OFFICE

The Contact Person or Office designated by the Lab as the person responsible for receiving complaints concerning this policy and for providing further information about matters covered by the Lab's HIPAA Notice of Privacy Practices is (*replace this with the name or title of designated Contact Person or Office*).

D. NOTICE OF PRIVACY PRACTICES

The Notice of Privacy Practices for the Lab is attached hereto at Exhibit B. The Notice of Privacy Practices shall be provided to any person upon request. In addition, the Notice of

Privacy Practices shall be posted prominently on any web site maintained by the Lab which web site provides information about the Lab's customer services or benefits.*

E. PROTECTED HEALTH INFORMATION ("PHI")

"Protected Health Information" ("PHI") includes any information that is created or received by the Lab in its role as a health care provider relating to past, present or future physical or mental health or condition of an individual, provision of health care, and/or future payment for the provision of health care and that identifies the individual or with respect to which there is a reasonable basis to believe that it could be used to identify the individual. PHI does not include employment records held by a Lab in its role as an employer.

PHI would include any information which relates to eyeglasses or the provision of eye care, from which one might reasonably identify the individual who is the subject of the such eye care. While it is unlikely that an optical lab would receive any information other than an individual's name, the range of possible PHI information includes the following:

- Patient's names.
- Patient addresses which include geographic subdivisions smaller than a state [including street address, city, county, precinct, certain zip codes . . . *See* § 164.514(b)(2) at Exhibit A hereto].
- All elements of dates (except for year) for dates related to the patient, including birth date, treatment date, and all elements of dates indicative of an age over 89.
- Telephone numbers.
- Fax numbers.
- E-mail addresses.
- Social security numbers.

---

* In the unlikely event that a patient deals directly with the Lab, the Lab shall provide the patient with a copy of the Notice of Privacy Practices, make a good faith effort to obtain a written acknowledgement of receipt, and document the acknowledgment or the good faith effort to secure the acknowledgment.

- Medical record numbers.
- Health plan beneficiary numbers.
- Account numbers.
- Certificates/license numbers.
- Vehicle identifiers and serial numbers, including license plate numbers.
- Device identifiers and serial numbers.
- Web site URLs.
- Internet protocol (IP) address numbers.
- Biometric identifiers including finger and voice prints.
- Full face photographic images.
- Any other unique identifying number, characteristic or code.

If health information is stripped of all of the above-described individual identifiers, then the Lab has no actual knowledge that the remaining information could be used to identify an individual, and the information does not constitute PHI. For example, a listing of prescriptions, or lens or frame types, without any other information, does not constitute PHI.

F. ALLOWED USE/DISCLOSURE/REQUEST OF PHI BY THE LAB

The Lab and its employees may only use, disclose or request PHI as expressly allowed in this policy.

1. Disclosure to the Patient – The Lab may disclose PHI about a patient to that patient upon request of the patient, without regard to the "Minimum Necessary" requirements described at Section G below.

2. Treatment Operations

a. Use within the Lab – The Lab may use among its personnel, PHI as part of its treatment operations. Treatment operations include the provision, coordination and management of the eyeglass services provided by the Lab. Such use and disclosure is subject to the "Minimum Necessary" requirements described at Section G below. For example, it is permissible that employees use and see PHI as part of their processing of orders, since the Lab has under Section G below, identified those class(es) of employees using PHI who have a reasonable need to do so, and has limited the amount of PHI which they use to that which they have a reasonable need to use.

b. Disclosures made to Other Health Care Providers for their Treatment Activities – The Lab may disclose PHI to other health care providers (e.g., eye care professionals, or coating labs) for their treatment activities. Such a disclosure by the Lab to another health care provider for its treatment activities is not subject to the minimum necessary rules described at Section G below.

3. As Part of Payment Operations – The Lab may disclose PHI to another health care provider (e.g., eye care professionals) or vision plan in order to receive payment from such entity. Such use and disclosure of PHI as part of an invoice or other payment activity is subject to the "Minimum Necessary" rules described at Section G below.

4. To Business Associates – The Lab may disclose PHI to a "Business Associate" if the Lab obtains satisfactory assurances from the Business Associate that it will appropriately safeguard the information; such assurances include having the Business Associate sign an agreement with specified Business Associate contract provisions. The Business Associate functions which trigger this rule typically involve contractors who assist with claims processing or administration, data analysis, quality assurance, billing, legal, or accounting. **Importantly, "Business Associates" do not include employees, and even more importantly the requirement to have Business Associates sign Business Associate contract provisions do not apply where a Lab discloses PHI to a health care provider for treatment of the patient, or where the Lab provides payment information to a vision plan**. For example, if the Lab provides PHI to an eye care professional in connection with fulfilling an order or to a coating lab to enable the coating lab to provide coating services, the Lab does not need to have the eye care

professional or the coating lab sign Business Associate contract provisions. If the Lab makes payment claims to a vision plan by electronic direct data entry or standard transaction entry to a third party clearinghouse, the Lab does not need a business associate contract with the clearinghouse. If the Lab uses a third party entity such as a remote order entry vendor website, or internet portal, to obtain PHI electronically from eye care professional customers, the Lab does not need a business associate contract with the clearinghouse. However, if the Lab uses a third party entity to provides software support, and that third party may access the Lab's computer system and PHI contained therein, and may even receive and analyze back up tapes with PHI, that third party will be a business associate of the Lab, and the Lab will have to require that third party to sign a business associate contract. In such a case, on in another event that the Lab provides PHI to a Business Associate in a situation which triggers the requirement for Business Associate contract provisions (e.g., the Business Associate will be performing for the lab claims processing administration, data analysis, billing, legal or accounting services), the prior written approval of the Lab Privacy Official shall be obtained, and the Lab Privacy Official shall have the Business Associate sign those of the Business Associate contract provisions at Exhibit C hereto as are deemed necessary and appropriate.

5. Other Uses – The HIPAA Privacy Regulations allow uses of PHI to be made in specified situations other than those listed in Section F (1-4) above. For example, disclosures of PHI is allowed where required by law; and disclosure of PHI is allowed for "marketing", but only if a specified authorization is obtained from the subject individual ("marketing" includes an arrangement between the Lab and any other entity whereby the Lab discloses PHI to the other entity in exchange for remuneration, so that the other entity may market products). Such use of PHI by the Lab to allow others to market, or for any purpose other than those listed in Sections F (1-4) above, is highly unlikely, and in any event may only be made with the prior written approval of the Privacy Official designated in Section B above, who may provide such approval only after obtaining any required authorizations.

G. USING/DISCLOSING OR REQUESTING PHI – ASSURING MINIMUM DISCLOSURE NECESSARY

1. Persons Accessing PHI – The Lab has identified at Exhibit D hereto those classes of lab employees who have a reasonable need to have access to PHI in order to carry out their duties, and for each such class of employees the types of PHI to which they need access. Those classes of employees listed in Exhibit D may use PHI within the Lab as is reasonably incident to the performance of their work. Disclosure by such employees of PHI to persons outside the Lab are governed by Section G (2) below.

2. Routine Disclosures of PHI – Set forth below are the disclosures of PHI which will be made on a routine and recurring basis by the Lab, and the procedures which will be followed to limit the PHI so disclosed to the minimum amount reasonably necessary to achieve the purpose of disclosure.

a. Disclosure of PHI to Health Care Providers (eye care professionals or coating labs) for part of their Treatment Operations – For example: (i) telephone inquiries concerning services requested, or the status or details of performance of such services; (ii) delivery of eyeglasses to eye care professionals, along with PHI - Such disclosures; if not part of a request for payment, are not subject to the Minimum Necessary requirements;

b. PHI Disclosed as part of Payment Operations – Invoice to health care provider (eye care professionals) or vision plan – Provide no more PHI in invoice to health care provider or vision plan than is requested by health care provider or vision plan, or that Lab can demonstrate is reasonably necessary. Any PHI above that requested by health care provider or vision plan, must be documented by a written memo sent to the Lab Privacy Official. Payment claims submitted electronically to vision plans which are compliant with the HIPAA Electronic Transaction Standards are considered to disclose only the minimum PHI necessary.

c. Other Routine and Recurring Disclosures of PHI

(i) Warranty/Return Claims - disclosure of PHI to a lens manufacturer to support a request for refund or replacement lens due to customer rejection may require a patient authorization. To avoid having to obtain such a patient authorization, the Lab must de-

identify the PHI provided to the lens manufacturer (for example, provide only the manufacturer's invoice number or the Lab's invoice number covering the rejected lens).

3. Non-Routine Disclosures – Before a Lab employee makes any non-routine or non-recurring disclosure of PHI [i.e., a disclosure of PHI other than one described in Section G (2) above], he/she must provide a written memo to the Lab Privacy Official explaining why it is necessary to disclose such PHI, and why the proposed disclosure is disclosing the minimum amount of PHI necessary. Such non-routine disclosure may only be made after receiving written approval from the Lab Privacy Official in response to such memo.

4. Routine Requests - Any Routine Request by the Lab for PHI shall be limited to that PHI which is reasonably necessary to accomplish the purpose of the request. The Lab anticipates making the following typical requests for PHI on a routine and recurring basis, and in such situations the PHI requested should be limited to that noted below in order to limit the amount of PHI requested to that amount reasonably necessary to accomplish the purpose for which the request is made:

a. Request by Lab of eye care professional for PHI in connection with processing and for fulfilling an order is a request in connection with treatment which may be made, and which is not subject to "Minimum Necessary" requirements of this Section G. The fact that the information may be obtained through a conduit such as a remote order entry vendor website, or internet portal does not change this fact.

5. Non-Routine Requests - Any request made by the Lab for PHI other than a routine request listed under Section G (4) above, may only be made after providing to the Lab Privacy Official a written memo describing the need for the request, and why the request is limited to the minimum amount of PHI reasonably necessary to accomplish the purpose of the request, and after the Lab Privacy Official has, in response to such memo, approved in writing the making of such request.

H. SAFEGUARDS

The Lab has the following administrative, technical and physical safeguards to protect PHI in its possession:

1. Training of all Lab employees as described in Section I below governing this Privacy Policy and HIPAA Privacy Requirements.

2. Limitation of the number of employees as set forth in Exhibit D hereto having access to PHI, to the minimum number reasonably necessary.

3. It is the Lab policy to prevent any unnecessary copying of PHI, and to limit those who may copy PHI to those individuals noted at Exhibit D hereto as having the need to copy PHI.

4. Storage, safekeeping, and disposal - when employees have completed use of PHI, it shall be placed and kept in an identified storage area to which only employees in classes listed in Exhibit D hereto have access. Where feasible, discarded information containing PHI shall be shredded or otherwise rendered unreadable.

I. TRAINING

1. All employees of the Lab will be trained on HIPAA Privacy Policy Compliance by no later than the later of April 14, 2003, or within a reasonable period of time, not to exceed two weeks, after a person joins the workforce.

2. All employees shall be provided access to this Privacy Policy no later than three days before their training date, and shall participate in training with the Lab Privacy Official or an individual designated by the Lab Privacy Official, to gain an understanding of this Privacy Policy and to answer any questions which the employee may have concerning such policy.

3. All employees having gone through such training, will sign a simple document acknowledging that they have been so trained, and the Lab Privacy Official shall retain the original of all such signed acknowledgments of training.

4. All employees shall be provided copies within one week of any amendments to this Privacy Policy, and those employee's whose duties are materially affected by the amendments shall be trained in those amendments.

J. PROCESS FOR HANDLING COMPLAINTS

1. Any person having a complaint concerning the Lab's Privacy Policy and procedures shall submit that complaint in writing to the Privacy Contact Person or Office designated pursuant to Section C above.

2. The Lab Privacy Contact Person or Office shall respond to such complaint in writing within two weeks if feasible, and in no event later than 30 days, setting forth any remedial action taken in response to such complaint, or explaining why no remedial action is justified. The Lab Privacy Official shall retain copies of all complaints so filed and all responses to such complaints.

K. SANCTIONS

1. Lab employees who fail to comply with this Privacy Policy shall be subject to sanctions, after an opportunity to meet with the Privacy Official and explain the reason for their failure to comply:

a. First Offense, Non-willful – Attend refresher training course within two months.

b. First Offense, Willful – Attend refresher training course within two months. Additional sanctions ranging from letter of reprimand in personnel file to termination, based upon severity of offense.

c. Subsequent Violations – Combination of required attendance at refresher training course and possible employee discipline ranging from letter of reprimand in file to termination of employment, based upon the number of previous violations, presence or lack of willfulness and other mitigating or aggravating circumstances.

L. MITIGATION

In the event that any Lab employee becomes aware of a violation of this Privacy Policy, the employee shall immediately notify the Lab Privacy Official in writing of the nature, cause and extent of the violation. The Lab Privacy Official shall take all reasonable measures to undo,

or if not possible to undo, then to minimize, the future use or disclosure of the PHI involved, and to correct the Privacy Policy procedures to avoid repetition of such violations.

M. NO RETALIATION

It is the absolute policy of the Lab not to intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against any individual for the exercise by the individual of any rights under this Privacy Policy or under HIPAA or for filing any complaint with HHS, or testifying, assisting or participating in any HHS investigation, compliance review, proceeding or hearing concerning HIPAA, or opposing any action which violates HIPAA, provided that such opposition has been taken in good faith, and the manner of such opposition is reasonable and does not involve a disclosure of PHI in violation of HIPAA.

N. NO WAIVER

The Lab shall not require any individuals to waive their rights to file complaints to HHS alleging non-compliance of the Lab with HIPAA, as a condition of their receiving services from the Lab.

O. RIGHTS OF PATIENTS TO REQUEST PRIVACY PROTECTION FOR PHI

1. Although the Lab does not anticipate that it will receive requests from patients to restrict use of disclosure by the Lab of PHI concerning the patient, the Lab shall permit patients to make such requests. The Lab is not required to agree to restrict its use of PHI beyond the restrictions imposed by the HIPAA Privacy Regulations, but it is the policy of the Lab to give consideration to such requests, and to accommodate such requests where in the sole discretion of the Lab it is reasonably feasible and not unduly burdensome to do so.

P. RIGHT OF PATIENTS TO ACCESS PHI

1. Although the Lab does not anticipate that the patients will make requests to inspect and obtain copies of PHI concerning them, the Lab recognizes that a patient has the right to inspect and obtain a copy of any PHI which the Lab may possess concerning the patient.

2. It is the policy of the Lab that any such request made by a patient must be made in writing and submitted to the Lab Privacy Official. The request shall be responded to within 30 days in accordance with the requirements of § 164.524(b) (copy attached at Exhibit A hereto).

Q. AMENDMENT OF PHI

1. Although the Lab does not anticipate that patients will make such requests, the Lab recognizes that a patient has the right to have the Lab amend PHI for as long as it is maintained by the Lab. The Lab may deny such a request if: (i) the Lab determines that the PHI which is the subject of the request was not created by the Lab, unless the patient provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment, or (ii) that the PHI would not be available for inspection, (iii) or that the PHI is accurate and complete. The Lab shall respond to such request within 60 days in accordance with § 164.526 (copy attached at Exhibit A hereto).

R. RIGHT TO AN ACCOUNTING OF DISCLOSURES OF PHI

1. The patient has the right to receive an accounting of disclosures of PHI made by the Lab in the previous six years, except for disclosures to carry out treatment, payment or health care operations. Note that this excludes disclosures made to eye care professionals for their treatment activities, or to supporting entities such as coating labs for their treatment (i.e., coating) activities, and it excludes disclosures made to eye care professionals and vision plans for payment purposes. The Lab shall respond to a request for an accounting within 60 days and in accordance with § 164.528 (copy attached at Exhibit A hereto).

2. The Lab shall document and retain documentation of all accountings which it is required to make. Such documentation must be retained for at least six years from the date of its creation. The Lab Privacy Official is responsible for receiving and processing requests for an accounting.