POLSINELLI

900 W. 48th Place, Suite 900, Kansas City, MO 64112 • 816.753.1000

April 27, 2022

Alexander D. Boyd
816-572-4470
816-753-1536
aboyd@polsinelli.com

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)

The Honorable John Formella
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of a Potential Data Security Incident

Dear Attorney General Formella:

We represent Allied Eye Physicians & Surgeons, Inc. ("Allied Eye"), 5250 Far Hills Ave., Kettering, OH 45420, in connection with an incident that occurred at one of Allied Eye's vendors that may have involved the personal information of six (6) New Hampshire residents. Allied Eye is reporting the incident pursuant to N.H. REV. STAT. ANN. § 359-C:20. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While Allied Eye is notifying you of this incident, Allied Eye does not waive any rights or defenses relating to the incident or this notice.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

Eye Care Leaders ("ECL") is a third-party service provider that stores Allied Eye's electronic medical records in ECL's cloud-based myCare Integrity EMR. On or about December 6, 2021, ECL notified Allied Eye that the myCare Integrity EMR was not available due to unspecified technical issues. The outage lasted until approximately December 15, 2021. On December 15, 2021, ECL stated that "On Saturday, December 4, an unknown attacker accessed the Integrity back-end and deleted some information." ECL stated that it was restoring its data from backups, that its investigation and review of the information was ongoing, and that it will notify Allied Eye if ECL finds "any lasting impacts to data, including PHI." According to ECL, the incident did not involve ransomware.

On March 1, 2022, ECL notified Allied Eye for the first time that the incident may have involved unauthorized access to personal information or protected health information. ECL stated that, although ECL "has not identified evidence confirming unauthorized access, acquisition, or

disclosure of PHI or PII, [ECL] also cannot rule out the possibility of such activity." Accordingly, ECL presumed that the third party may have accessed or acquired information stored within ECL's myCare Integrity EMR. This information included, depending on the individual, names, addresses, dates of birth, Social Security numbers, and medical treatment and diagnosis information. As a result, out of an abundance of caution, Allied Eye is notifying all of its patients who had protected health information or personal information stored in the myCare Integrity EMR. Allied Eye does not have any evidence of harm as a result of this incident.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

Allied Eye determined that the incident potentially involved six (6) New Hampshire residents and is notifying the involved individuals via written notification today. This notice includes a contact number the individuals can call should they have questions or require assistance. Allied Eye is also providing the individuals with an offer of a complimentary one-year membership of Experian IdentityWorks Credit 3B. A copy of the notice that was sent to the involved individuals is enclosed.

STEPS TAKEN RELATING TO THE INCIDENT

The incident occurred at ECL, a third-party service provider to Allied Eye. ECL advised Allied Eye that upon discovering the incident, ECL contained the incident, notified law enforcement, conducted an investigation, and restored data from available backups. ECL assured Allied Eye that ECL has implemented additional security measures to lessen the likelihood that an incident like this will occur in the future, including reviewing and updating access controls and permissions, reviewing and updating data storage security procedures, strengthening network protections, improving server patching and data backup processes, and onboarding additional internal and third-party technical resources and monitoring personnel. Finally, Allied Eye is notifying potentially involved New Hampshire residents, providing them free credit monitoring services, and providing them with information on how they can protect themselves against fraudulent

activity and identity theft.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Alexander D. Boyd

Enclosure

Allied Eye Physicians and Surgeons, Inc.

Marshall Wareham, M.D

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

RE: NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Allied Eye Physicians & Surgeons Inc. ("Allied Eye") values and respects the privacy of your information, which is why we are writing to advise you of a recent incident that occurred at one of our vendors that may have involved some of your personal information. While we do not have any evidence that your information has been misused, we are writing to advise you about the incident as required by law, and to provide you with guidance on steps you can take, should you feel it is appropriate to do so.

What Happened? Allied Eye uses Eye Care Leaders ("ECL"), a third-party service provider, to store electronic patient medical records and related information. ECL recently notified us and many other eyecare providers that on December 4, 2021, an unknown third party accessed its network and may have deleted certain files stored by ECL in ECL's myCare Integrity Electronic Medical Records ("EMR"). ECL advised us that upon discovering the incident, ECL contained the incident, notified law enforcement, conducted an investigation, and began restoring data from backups where available. On March 1, 2022, ECL further notified us that, although ECL has not identified evidence confirming unauthorized access, acquisition, or disclosure of any personal information or protected health information, ECL cannot rule out the possibility that the third party may have accessed or acquired information stored within ECL's myCare Integrity EMR. As a result, out of an abundance of caution, and as required by law, we are notifying all of our patients who had personal information stored by myCare Integrity EMR. We do not have any evidence of harm as a result of this incident.

What Information Was Involved? To the extent your information was stored in ECL's myCare Integrity EMR, the incident may have involved unauthorized access or acquisition of your name, address, telephone number, date of birth, Social Security number, and medical treatment and diagnosis information.

What We Are Doing. We are reviewing our relationship with ECL and the technical controls they have in place for securing our patients' information. ECL has assured us that it has engaged third party experts and implemented additional measures to secure and monitor its environment. Although we are not aware of any instances of fraud or identity theft involving your information, we are offering a complimentary one-year membership of Experian IdentityWorks^{SM} Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

What You Can Do. While we have no evidence that your personal information has been misused, we encourage you to take advantage of the complimentary credit monitoring included in this letter. You can find more information on steps to protect yourself against identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience this incident might cause. For further information and assistance, please call 1-???-???-???? Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

Marshall Wareham, M.D.
Owner/President of Allied Eye Physicians and Surgeons, Inc.

ACTIVATING YOUR COMPLIMENTARY CREDIT MONITORING

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **<<b2b_text_6(activation deadline)>>** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code**: **<<activation code s_n>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number **<<b2b_text_1(engagement number)>>** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

This notice was not delayed by law enforcement.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; https://ag.ny.gov/consumer-frauds/identity-theft; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.