Health
AUGUSTA UNIVERSITY

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

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We recently were notified by Eye Care Leaders ("ECL") that an ECL data security incident may have involved some of your personal information. ECL is an outside vendor that hosts the electronic medical records ("EMR") system ***only for ophthalmology services***. The Ophthalmology EMR is called ECL myCare Integrity.

What happened? On March 28, ECL provided us with the following information about the ECL myCare Integrity EMR Ophthalmology security incident, which was sent as update to prior notice of ongoing investigation: On or around December 4, 2021, attacker(s) accessed the Integrity back-end hosted on Amazon Web Services (AWS) and deleted databases and system configuration files. The activity was detected in less than twenty-four (24) hours, and ECL's incident response team contained and began investigating the incident. ECL began efforts to restore deleted databases from backups to limit impact to the availability of the Ophthalmology EMR. Work is ongoing to determine whether the remaining, unrestored databases can or need to be restored. Although investigators have not identified any evidence of data exfiltration, there is insufficient evidence to allow ECL investigators to conclude that exfiltration could not have occurred during the attack.

What information was involved? ECL provided general information about the personal information that may have been impacted. ECL has not identified evidence confirming unauthorized access, acquisition, or disclosure of your specific personal information, but ECL also cannot rule out the possibility of such activity. Information stored in an Ophthalmology EMR varies widely by individual, but may have included things such as your name, contact information, social security number, insurance information, and ophthalmology-related or other health information. ***NOTE: This incident did not occur on AU Medical's campus and did not affect student records or the Hospital's primary electronic medical record system. This incident was limited to ophthalmology records housed on the ECL's outside, vendor-hosted Ophthalmology EMR.***

What are we doing in response? AU Medical is assessing alternative ophthalmology EMRs and providing this notice to you in as a precaution. ECL has stated that ECL has "taken measures to enhance our technical, administrative, and physical safeguards to further secure Integrity against attack. To date, [ECL has] implemented a broad range of improvements to strengthen Integrity's security, including: 1. Reviewing and updating access controls and permissions, 2. Reviewing and updating data storage security procedures, 3. Strengthening network protections, 4. Improving server patching and data backup processes and 5. Onboarding additional internal and third-party technical resources and monitoring personnel."

What you can do? We have not had any reports of identity theft associated with the ECL incident and do not anticipate any such reports. In an abundance of caution, **AU Medical is offering you one (1) year(s) of *free* credit monitoring and identity theft insurance through Experian - to give you peace of mind. *You must activate the free product by the activation date in order for it to be effective. The activation instructions are included with this notification.* We also have included some additional steps that you can take, as appropriate.**

For more information about this incident, please call toll free 1-???-???-???? between the hours of 9 am to 6:30 pm ET Monday - Friday (excluding holidays). We sincerely apologize for any concern this may have caused you.

Sincerely,

Allison K. Luke
AVP, Compliance and Privacy

ELN-14335

STEPS YOU CAN TAKE

Below is information on steps you can take to protect yourself.

• **ACTIVATE Your FREE Experian IdentityWorks Product NOW in Three Easy Steps.** To help protect your identity, we are offering you a **complimentary one (1) year membership** of Experian's IdentityWorks product. This product helps detect possible future misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks Alert is completely free to you and enrolling in this program will not hurt your credit score.

1. **ENSURE You Enroll By**: <<b2b_text_6(activation deadline)>> **(Your code will not work after this date.)**
2. **VISIT** the **Experian IdentityWorks website** to enroll: <<URL>> **PROVIDE Your Activation Code:** [redacted]

If you have questions about the IdentityWorks or need an alternative to enrolling online, **please call 877-288-8057** and provide engagement <<b2b_text_1(engagement number)>>. A credit card is not required for enrollment. Once your IdentityWorks membership is activated, you will receive the following features:

- **Experian Credit Report at Signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Restoration Agents are immediately available to help address credit/non-credit related fraud.
- **$1 Million Identity Theft Insurance:**[2] Provides coverage for certain costs and unauthorized electronic fund transfers.

You must activate your membership by the Enrollment Date (noted above) by enrolling at https://www. <<URL>> **or calling 877-288-8057 to register your activation code above in order for this service to be activated.** Once your enrollment in IdentityWorks is complete, carefully review your credit report for inaccurate or suspicious items. 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 team at 877-288-8057.

• **FREEZE YOUR CREDIT FILE.** You have a right to place a 'security freeze' on your personal credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a freeze to take control over who gets access to the personal/financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made regarding a new loan, credit, mortgage, or any other account involving extension of credit. Security freeze generally does not apply to existing account relationships and when a copy of your report is requested by existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a freeze. To place a security freeze on your credit report, contact each of the following credit bureaus and clearly explain in the call/letter that you are requesting a security freeze:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

To request a security freeze, provide your full name (middle initial, Jr., Sr., II, III, etc.), Social Security Number, date of birth; home addresses over the past 5 years; proof of current address such as a current utility bill or telephone bill; photocopy of government issued identification card (driver's license or ID card, military ID, etc.); and if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. If you request a security freeze via toll-free telephone or other secure electronic means, credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the agencies have 3 business days after receiving your request to place a security freeze on your credit report. Credit agencies must also send written confirmation within 5 business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze. To lift the freeze

[1]Offline members will be eligible to call for additional reports quarterly after enrolling.
[2]Experian underwriting footnote

to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and PIN or password provided when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift freeze for those identified entities or for the specified period of time. To remove the freeze, you must send a written request to the 3 credit bureaus by mail and include proper identification (name, address, & social security number) and PIN number or password provided when you placed the freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

• **PLACE FRAUD ALERTS ON YOUR ACCOUNT / CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your bank account and/or personal credit file. An initial credit file fraud alert is a 1-year alert that is placed for free on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is an alert lasting 7 years. Contact the 3 credit reporting agencies listed above to activate an alert.

• **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS & REPORT FRAUD. CHANGE PASSWORDS AND SECURITY VERIFICATION QUESTIONS & ANSWERS.** Always carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity, changing passwords/security verifications as needed – particularly if same password is used over multiple online accounts. If your medical information was involved, it is also advisable to review the billing statements you receive from your healthcare providers. Report suspicious or fraudulent charges to your insurance statements, provider billing statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor, healthcare provider and law enforcement, including FTC and/or your State Attorney General.

• **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-322-8228 to obtain 1 free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the 3 credit reporting agencies directly to obtain such additional reports.)

• **POLICE REPORT:** You have a right to a police report about this incident (if any exists). If you're an identity theft victim, you have the right to file a police report and obtain a copy of it. Notification of this incident has not been delayed as a result of a law enforcement investigation.

• **FAIR CREDIT REPORTING ACT (FCRA):** Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552. 1) You must be told if information in your file has been used against you. 2) You have the right to know what is in your file. 3) You have the right to ask for a credit score. 4) You have the right to dispute incomplete or inaccurate information. 5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. 6) Consumer reporting agencies may not report outdated negative information. 7) Access to your file is limited. 8) You must give your consent for reports to be provided to employers. 9) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. 10) You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. 11) You may seek damages from violators. 12) Identity theft victims and active duty military personnel have additional rights.

• **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT, FRAUD ALERTS, SECURITY FREEZES AND FCRA FROM THE FEDERAL TRADE COMMISSION.** Go to http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for additional information. Federal Trade Commission also provides information at www.ftc.gov/idtheft FTC hotline is 877-438-4338; TTY: 1-866-653-4261 or write to FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.

• OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM YOUR STATE ATTORNEY GENERAL.

- *Maryland: You may contact and obtain information from your state attorney general at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-410-528-8662; www.oag.state.md.us Consumer Hotline1-410-528-8662, or consumer@oag.state.md.us.*
- *Connecticut: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag*
- *District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001, 1-202-727-3400, databreach@dc.gov, www.oag.dc.gov.*
- *Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html*
- *New York: You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-4748583 / 1-800-6971220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov*
- *North Carolina: You may contact and obtain information from your state attorney general at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699, 1-919716-6000/ 1-877-566-7226, www.ncdoj.gov*
- *Rhode Island: Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401274-4400, www.riag.ri.gov. (Approximately <<INSERT NUMBER>> Rhode Island residents were impacted by this incident.)*