Posted May 27, 2022

Public Website Notice of Eye Care Leaders' (Vendor) Data Security Incident

Eye Care Leaders ("ECL") recently notified AU Health that ECL has experienced a data security incident – relating to certain ophthalmology records. ECL is an outside vendor that hosts our electronic medical record ("EMR") system ***for ophthalmology services only***. ECL's proprietary Ophthalmology EMR is called ECL myCare Integrity.

ECL provided AU Health with a March 28 update to prior notice of ongoing investigation and stated all the following information about its ECL myCare Integrity Ophthalmology EMR:

> ECL's myCare Integrity back-end hosted on Amazon Web Services was inappropriately accessed on approximately December 4, 2021, and attacker(s) deleted databases and system configuration files.
>
> The activity was detected by ECL 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 in order to limit impact to the availability of the Ophthalmology EMR.

ECL further stated that, although ECL investigators have not identified any evidence of data exfiltration, there was insufficient evidence to allow ECL investigators to conclude that exfiltration could not have occurred during the attack.

Upon notice that certain ophthalmology patients might be affected, AU Health promptly conducted a thorough investigation to ascertain all potentially affected patients in order to be able to provide notice to individuals - as a precaution.

Notices are being mailed to the last known address and should be received over the next week.

ECL has stated that ECL has "taken measures to enhance [its] 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."

Notwithstanding, we are assessing alternative ophthalmology EMR platforms.

ECL was not able to provide specific information about the personal information that may have been impacted. Information stored in an Ophthalmology EMR varies widely by individual, but may have included things such as name, contact information, social security number, insurance information, health

and ophthalmology-related information. ECL stated it has not identified evidence confirming unauthorized access, acquisition, or disclosure of specific individuals' personal information.

IT IS IMPORTANT TO NOTE:

- ***The ECL incident did <u>not</u> occur on AU Medical campus and did <u>not</u> affect student records, employee records, or the Hospital's primary electronic medical record system.***

- ***This incident was limited to <u>ophthalmology records</u> (primarily clinic records) housed outside of AU Health IT systems by ECL on a specialized Ophthalmology EMR platform.***

We are not aware of any reports of identity theft associated with ECL's security incident, and do not anticipate any such reports. In an abundance of caution, AU Medical is offering <u>*free*</u> credit monitoring and identity theft insurance to give potentially affected ophthalmology patients peace of mind.

Ophthalmology clinic patients who have questions and/or need additional information about the ECL incident may email ECLVendorDataIncident@nelsonmullins.com or call toll-free 1-800-298-2295 between the hours of 9 am to 6:30 pm ET Monday - Friday (excluding holidays). Please send or leave a message with your contact information and questions, and someone will email or call you back as soon as possible.

We sincerely apologize for any concern this may have caused our ophthalmology patients.