

## Stokes Regional Eye Centers Provides Notice of Data Privacy Incident at Third-Party Vendor

**Florence, SC – June 17, 2022** - Stokes Regional Eye Centers (“Stokes”) is providing notice of an event that occurred with one of our third-party vendors, Eye Care Leaders (“ECL”), which may affect the privacy of information. ECL operates and manages Stokes’ electronic medical record (“EMR”) system through its myCare Integrity software.

**What Happened?** On December 8, 2021, Stokes discovered that it was unable to access the EMR hosted on ECL’s systems. Stokes immediately engaged with ECL’s support team to troubleshoot the issue and took steps to ensure patient care could continue uninterrupted. Functionality to the EMR was restored after a week and Stokes received no additional information regarding this outage until March 1, 2022. On March 1, 2022, ECL notified Stokes that this outage was the result of an unauthorized actor gaining access to ECL’s systems on December 4, 2021, and deleting certain records within the system. Based on this notice, Stokes launched an investigation. On April 19, 2022, Stokes received additional information from ECL relating to this event and the investigation. Unfortunately, based on this information, ECL was unable to determine if patient information was accessed or acquired by the unauthorized actor as a result of this event. There is currently *no evidence* that this event involved any of Stokes internal systems and all evidence suggests that this event occurred only on ECL’s systems.

**What Information Was Involved?** As the investigation was unable to determine if your information was accessed or acquired as a result of this event, Stokes is taking steps to notify you out of an abundance of caution. The impacted involves your patient file, which could include your name, address, Social Security number, date of birth, government issued identification number, medical information, and health insurance and billing information. To date, ECL has not reported any actual or attempted misuse of this information to Stokes.

**What We Are Doing.** Stokes takes this incident and the security of information within our care very seriously. Upon being notified of this incident, Stokes immediately launched an investigation to determine the nature and scope of this incident. As part of our ongoing commitment to the privacy of information in our care, Stokes is reviewing existing security policies and procedures regarding our third-party vendors and are working to evaluate additional measures to further protect against similar incidents moving forward. Stokes will also be notifying state and federal regulators, as required. In addition, Stokes is offering credit monitoring and identity theft protection services through Equifax.

**For More Information.** Stokes understands that you may have questions that are not addressed. If you have additional questions, please call the dedicated assistance line at (855) 965-5775, which is available Monday through Friday, between the hours of 9:00 a.m. and 9:00 p.m. Eastern Time, or write to Stokes at 367 West Evans Street, Florence, SC 29501. Stokes recommends that potentially impacted individuals follow the recommendations in the letter they received and contact the call center with any questions.

**What You Can Do.** Stokes encourages everyone to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name

without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

**Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

**TransUnion**

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

**Equifax**

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. 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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed 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 a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

**Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

**TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity

theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.