On September 1, 2022, we learned that cyber criminals had gained unauthorized access into various components of the OakBend Medical Center ("OakBend") computer network and that certain servers and computers were encrypted. Immediately upon learning about this access and encryption, on the morning of September 1, 2022, we took action to remediate this incident and harden our system against future attacks.

While we know that the cybercriminals had sufficient access to OakBend's systems to encrypt our data, our investigation indicates that a limited amount of data was actually transferred out of the OakBend computing environment. For example, we do not believe that the cybercriminals were able to remove the entire medical record of OakBend's patients. It does appear, however, that the cybercriminals were able to access and/or remove certain employee data sets and certain reports that included the personal and medical information related to our current and former patients, employees, and related individuals. In some instances, this information may have included the name, contact information (such as street and email address), social security number, and date of birth for the impacted individuals.

OakBend Medical Center conducted a thorough review of the incident, and our IT team has worked diligently to restore the integrity of our network. We also reported the incident to law enforcement and are cooperating with the FBI to investigate the cybercriminals. Furthermore, we have implemented additional security measures designed to prevent a recurrence of such an attack and to protect the privacy of our patients, employees, and community members.

OakBend has sent notification letters to individuals that we believe might have been affected. If you are a former patient or employee or otherwise think you may have been affected and did not receive a letter, please contact questions@obmc.org. You will be asked to provide further information so that we can determine whether you might have been affected in this incident. OakBend will be offering certain identity theft protection services to affected individual for a limited period of time.

It is possible you may receive spam email messages and/or other fraudulent communications using your contact information. We want to urge you to be cautious when opening links or attachments from unknown third parties. Be particularly careful if you receive emails asking for your login/password information at various financial institutions and/or from the IRS, as such emails are likely fraudulent.

We further recommend that you remain vigilant by reviewing your account statements and 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 also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission. Of course, it is always a good idea to change your passwords regularly.

For more information regarding identity theft, the toll-free numbers and addresses of the major credit reporting agencies, and ways you can help to protect yourself, please see Page 2.

If you have any questions or require assistance, please call toll-free (855) 519-2341, or email questions@obmc.org.

Information About Identity Theft Protection

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

It is important that you remain vigilant by reviewing your account statements and credit reports closely. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax:	P.O. Box 740241, Atlanta, Georgia 30374-0241, 1 866-349-5191, www.equifax.com
Experian:	P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion:	P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion

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 also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission ("FTC").

Place A Fraud Alert On Your Credit Report

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax:	1-800-525-6285, www.equifax.com
Experian:	1-888-397-3742, www.experian.com
TransUnion:	1-800-680-7289, fraud.transunion.com

Place A Security Freeze on Your Credit File

You have the right to place a security freeze on your credit file free of charge. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. In addition, you may incur fees if you acquire certain other services that might be offered by the credit reporting agencies. Check with the applicable credit reporting agency for relevant details. 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 may differ, please contact the three major credit reporting companies as specified below to find out more information:

Equifax:	1-888-298-0045, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Additional Free Resources on Identity Theft

For more information on identity theft, fraud alerts, and security freezes, you may wish to review information provided by the FTC at www.ftc.gov/idtheft, or you can contact the FTC by calling 1-877-ID-THEFT (877-438-4338), or writing to 600 Pennsylvania Avenue, NW, Washington, DC 2058