Oaklawn
Real People. Real Care.

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

[redacted]

<<b2b_text_1 (Header)>>

Dear [redacted]:

The privacy and security of the personal information we maintain is of the utmost importance to Oaklawn Hospital. We are writing with important information regarding a recent data security incident that may have involved some of your information. We want to provide you with information about the incident, explain the services we are providing to you, and let you know that we continue to take signif cant measures to protect your information.

What Happened?

Oaklawn Hospital was the target of an email phishing campaign that resulted in a limited number of employees receiving a suspicious email containing a malicious link. These employees unfortunately fell victim to the phishing campaign, resulting in an unauthorized individual gaining access to those employees' email accounts. Upon learning of the incident, Oaklawn Hospital disabled the impacted email accounts and required mandatory password resets to prevent further misuse.

There is no evidence that the purpose of the phishing campaign was to obtain patient information and we have no evidence that any of your information was actually acquired or used by the unauthorized individual. However, out of an abundance of caution, we are providing notice and of ering you identity monitoring services at no charge.

What We Are Doing.

Upon learning of this issue, we immediately commenced a thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals. After an extensive forensic investigation and comprehensive manual document review, we discovered on July 28, 2020 that one or more of the email accounts that were accessed between April 14, 2020 and April 15, 2020 may have contained some of your personal and/or protected health information.

Since the date of this incident, we have taken several steps to implement additional technical safeguards on our email system to prevent the recurrence of similar incidents. We have also implemented additional training and education for our employees to increase awareness of the risks of malicious emails, including how employees can identify and handle malicious emails.

What Information Was Involved.

The impacted email account(s) may have contained some of your protected health information, including your [redacted]. Your Social Security number and f nancial information **were not** included in the information that may have been accessed.

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we have chosen to make you aware of the incident. We recommend that all patients and personal representatives of patients monitor insurance statements for any transactions related to care or services that have not actually been received. We are also including a list of steps that can be taken to help protect your medical information.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit f les, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your f nancial account statements and credit reports for fraudulent or irregular activity on a regular basis. We are also of ering steps you can take to protect your medical information on the following pages.

For More Information.

Please accept our apologies that this incident occurred. We have taken necessary steps to prevent this from happening again. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it and to prevent subsequent occurrences. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and conf dential toll-free response line that we have set up to respond to questions at 1-888-974-0058. This response line is staf ed with professionals familiar with this incident and knowledgeable on what you can do if you are concerned about potential misuse of your information. The response line is available Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

Gregg Beeg
Chief Executive Of cer
Oaklawn Hospital

Protecting Your Medical Information.

The following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benef ts statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benef ts statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a benef ciary. Follow up with your insurance company or the care provider for any items you do not recognize.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Of ce to report suspected incidents of identity Theft: Of ce of the Attorney General of Iowa, Consumer Protection Division, Hoover State Of ce Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Of ce: Of ce of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Of ce: Of ce of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-775 (TDD/TYY Support: 800-788-9898); Medicare Fraud Control Unit Direct Line: 212-417-5397.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Of ce: Of ce of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.