MOREHEAD
MEMORIAL·HOSPITAL

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Dear <<MemberFirstName>> <<MemberLastName>>,

Morehead Memorial Hospital takes the privacy and protection of personal information very seriously. We recently experienced a cybersecurity incident involving patient and employee data. It is important to us that we let you know about this incident so that you can take steps to protect yourself.

What Happened

An unauthorized party sent fraudulent communications to Morehead, enabling them to obtain login information that allowed access to two email accounts within the hospital. Promptly upon learning about these communications, steps were taken to address the incident. Our IT staff cut off access to the affected accounts, issued a network-wide password reset, and engaged top-tier forensic consultants to conduct a full investigation. We have contacted the FBI and the Department of Homeland Security and will cooperate with their investigation.

What Information Was Involved

The email accounts contained certain types of information about our patients and employees. <<ClientDef1(Breach Details Variable Text)>><<ClientDef2(Breach Details Variable Text)>> (Your name, health insurance identifiers or information related to payments made for medical services, financial account details, credit or debit card numbers, and information about medical treatments, diagnoses, or services received were affected.)

Please be assured that at this time we are not aware of any fraud or misuse of your information as a result of this incident.

What We Are Doing

To help prevent an incident like this from recurring, we are enhancing additional security measures to protect our systems, and we are providing additional training to our staff so that they are better prepared to identify potentially fraudulent communications. We have also created an internal web page to provide timely updates to employees as we become aware of phishing and email attacks.

Out of an abundance of caution, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Web Watcher, Fraud Consultation, and Identity Theft Restoration. For more information about these services and instructions on enrolling, please see the enclosed reference guide "Information About Identity Theft Protection." It is important to state again that, at this time, we are not aware of any misuse of your information.

What You Can Do

Patients who have received medical services provided by Morehead, or individuals who are members or beneficiaries of the hospital's group health plan, should regularly review their explanation of benefits (EOB) statements. If services listed on the EOB were not received by any plan beneficiary, you should immediately contact the health plan.

Although your Social Security number was not affected by this incident, as a general precaution you can carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office to file a police report for identity theft and get a copy of it. Copies of the police reports are often requested by creditors.

You will find more advice in the enclosed "Information About Identity Theft Protection" reference guide. It describes further steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission and the Department of Health and Human Services regarding identity theft protection and details about placing a fraud alert or a security freeze on your credit file.

For More Information

For more information about this incident, please call 1-833-202-7408, Monday through Friday from 9 a.m. to 6 p.m. Eastern Time. You will also find information on Morehead's Website at http://morehead.org/data-incident. Protecting your information is important to us, and we regret any concerns that this matter may cause.

Sincerely,

Dana M. Weston
President & CEO
Morehead Memorial Hospital

Information About Identity Theft Protection

Activating Your Identity Monitoring Services: To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until **January 18, 2018** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-833-202-7408. Please have your Membership Number ready.

The Kroll identity monitoring services include the following features:

- **Web Watcher.** Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.
- **Fraud Consultation.** You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.
- **Identity Theft Restoration.** If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

Review of Accounts and Credit Reports: As a precaution you may regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You can 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 at the end of this guide.

Remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the relevant government institution and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft. There may be similar resources available at the state level, and you may contact your state department of revenue directly for more information.

Residents of North Carolina may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

Information About Medical Identity Theft: Patients and employees who pay for medical services can regularly review the explanation of benefits (EOB) statements that they receive from their health insurers or health plans. If they identify services listed on the EOB that were not received, they should immediately contact the health plan. For more information about protecting yourself from the Department of Health and Human services, please visit https://oig.hhs.gov/fraud/medical-id-theft.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may request an initial fraud alert if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may request an extended fraud alert 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 contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. 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 differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:
P.O. Box 740256, Atlanta, GA 30374
877-478-7625

Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
P.O. Box 1000
Chester, PA 19016
800-888-4213

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872