EMORY
HEALTHCARE
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name1>>:

At Emory Healthcare (EHC), our top priority is providing the highest quality healthcare possible. EHC values and respects your privacy, which is why we are writing to advise you about an incident involving some of your medical information. We also want to share the steps we have taken since discovering the incident, and to provide guidance on what you can do to protect yourself.

Please note this incident ***did not*** involve your Social Security number, driver's license number, address, phone number, credit card information or any of your financial information.

EHC recently learned that some EHC patients' protected health information was located on a University of Arizona College of Medicine (UA) Microsoft Office 365 OneDrive account. A OneDrive account is an Internet-based data storage system. The files were obtained and placed on the account by a former EHC physician, without EHC's authorization. The physician is currently employed by the UA. Based on information disclosed to us by the UA from their investigation, it is our understanding that the information may have been accessible to individuals that were set up with a specific type of UA e-mail account, but there is no indication that the information was accessed or used in any way while on the OneDrive Account. Additionally, some of the information may have been available to several other former EHC physicians currently employed at UA and limited UA staff and those at UA investigating this matter.

UA took immediate action to remove the information from the OneDrive account and hired a third-party forensic firm to review the account. On October 18, 2017, EHC received a list of the files that were located on the OneDrive Account and subsequently launched an investigation. We determined that some of your information was on the Account. The files contained medical information primarily from radiology services provided to patients from 2004 through 2014 and included patients' names and, in some cases, dates of birth, dates of service at EHC, provider names, medical record numbers, diagnostic/treatment information and treatment locations. All EHC patient information has been expunged from all UA systems, and we believe the potential for future misuse of your information related to this incident is unlikely.

If you have any additional questions, you may call our confidential inquiry line at 877-494-9830 toll-free, between 9 a.m. and 9 p.m., Eastern Time, Monday through Friday.

We are sincerely sorry that this situation occurred and for any concern it may cause you. EHC is committed to the privacy and security of our patients' information. We are closely reviewing this matter and will further review and work to enhance our security measures and patient care team education programs to help prevent something like this from happening in the future.

Sincerely,

Jonathan S. Lewin M.D.

Jonathan S. Lewin, MD, FACR
President and Chief Executive Officer
Emory Healthcare

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring 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 should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: If you are a Georgia resident, you are entitled to three (3) credit reports from each reporting agency per year. To request your free annual reports, which would be sent to you by mail, you must contact the three (3) main national credit reporting agencies listed below.

If you are not a Georgia resident, you may obtain a free copy of your credit report once every twelve (12) months from each of the three (3) national credit reporting agencies by visiting http://www.annualcreditreport.com, by calling toll free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at: https://www.annualcreditreport.com/cra/requestformfinal.pdf.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three (3) national credit reporting agencies. Contact information for the three (3) national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax
1-800-349-9960
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion
1-888-909-8872
www.transunion.com
P.O. Box 2000
Chester, PA 19022

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least ninety (90) days. The alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at http://www.annualcreditreport.com.

Credit and Security 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 on your credit file, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may cause a delay should you attempt to obtain credit. In addition, you may incur fees for placing, lifting and/or removing 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:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

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

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft at:

Office of the Attorney General
220 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
www.ncdoj.com

Rhode Island Residents: We believe that this incident affected one Rhode Island resident. You can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400