



URGENT — Please Open Immediately.

<<Firstname>> <<Middlename>> <<Lastname>>
<<Address1>>
<<Address2>>
<<City>>, <<Stateprovince>> <<Postalcode>>
<<Intelligent Mail Barcode>>

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

Dear <<FirstName>> <<MiddleName>> <<LastName>>,

Emory Healthcare is dedicated to serving your health care needs, and that includes preserving the confidentiality and privacy of our patients. If we are ever concerned that your information may be at risk, it is our obligation to conduct a thorough investigation and inform any patients who may be affected. We were recently informed of an incident that involves your personal information. The details of this incident and the special services we are offering to protect you are noted below.

On February 20, 2012, we discovered that 10 backup data discs containing information from some of our surgical patients, prior to May 2007, were missing from their storage location in a surgery support office at Emory University Hospital. As soon as we discovered the discs were missing, we launched an extensive search and investigation, and we are continuing those efforts. At this point, we believe this was a result of human error. There is no indication that this information has been or will be used for malicious intent. It is also important to note that this incident was not a breach or any sort of "hacking incident" of our electronic medical records or other systems.

The investigation revealed the discs were removed sometime between February 7 and February 20, 2012. They contained data from a deactivated software system that was discontinued in 2007, but may have contained the following personal information: name, address and date of birth. Your Social Security number may also have been included on the discs. Approximately 228,000 of the records included Social Security numbers; there were approximately another 87,000 records that did not include Social Security numbers.

The following clinical information may also have been included: date of surgery, diagnosis, procedure code or the name of the surgical procedure, device implant information, surgeon's name and anesthesiologist's name. The information is related to patients treated at Emory University Hospital, Emory University Hospital Midtown and The Emory Clinic Ambulatory Surgery Center between September 1990 and April 2007. It did not contain information for patients treated at any other Emory Healthcare facility.

We assure you that we are committed to safeguarding your personal information and have taken immediate steps to fortify the protective measures that are already in place. New and enhanced data control measures have been implemented accordingly.

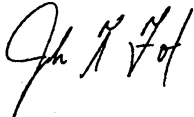
To provide you additional protection and to further assist you, we recommend that you register for credit monitoring services with Kroll, Inc., which we have arranged to offer to you personally at no charge to you for one year. The attached Kroll Service Reference Guide provides information on how you can register and recommendations by the U.S. Federal Trade Commission on how to further protect your personal information. For example, you also may want to place a fraud alert on your entire credit file. We have also included Enhanced Identity Theft Consultation and Restoration services for one year through Kroll should you need them.

We take our obligation to safeguard personal information very seriously and, therefore, we are alerting you so you can take steps to further protect yourself. We encourage you to remain vigilant and to carefully review your account statements and monitor your credit reports. You are entitled under U.S. law to one free credit report annually from each of the three national credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228.


If you have any additional questions or believe you suspect an identity theft issue, you may call the Emory Healthcare Support Center at 1-855-205-6950, 9 a.m. to 6 p.m. (Eastern Time), Monday through Friday.

Again, we sincerely regret this situation and any anxiety or inconvenience this may cause you. We hope that the support services offered to you help demonstrate our commitment to protecting your information and the value we place on our relationship as your health care provider.

Sincerely,



John T. Fox
President & CEO
Emory Healthcare



Anne Adams
Chief Privacy Officer
Emory Healthcare

<<FirstName>> <<MiddleName>> <<LastName>>
Membership Number: <<MembershipNumber>>

Member Services: 1-855-205-6950

9:00 a.m. to 6:00 p.m. (Eastern Time), Monday through Friday

If you have questions or feel you may have an identity theft issue,
please call ID TheftSmart member services.

Reference Guide

Kroll's ID TheftSmart Service™.

Because securing your personal information is important, Emory Healthcare has engaged Kroll Inc. to provide its ID TheftSmart service at no cost to you for one year should you choose to use them. Through this service, you have access to:

Enhanced Identity Theft Consultation and Restoration. Licensed Investigators, who understand the problems surrounding identity theft, are available to listen, to answer your questions, and to offer their expertise regarding any concerns you may have. And should your name and credit be affected by this incident, your investigator will help restore your identity to pre-theft status.

Continuous Credit Monitoring. Monitoring alerts make you aware of key changes in your credit file that could indicate the kind of unauthorized activity commonly associated with identity theft and fraud.

Please see the enclosed brochure for easy, simple instructions to take advantage of Kroll's services. To receive online credit services, please visit www.idintegrity.com to complete your authorization. If you would prefer to order and receive your credit services through the mail, please fill out and return the enclosed *Consumer Credit Report and Credit Monitoring Authorization Form*.

Note, however, that if you fill out and return the authorization form to receive credit services through the mail, you cannot sign up online.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity. You may also call the Emory Healthcare Support Center to be put in touch with Kroll's Licensed Investigator to answer your questions and assist you in resolving any issues.

Contact the U.S. Federal Trade Commission. If you detect any unauthorized transactions in your financial account, promptly notify your payment Card Company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities and the FTC. If you believe your identity has been stolen, the FTC recommends that you take these additional steps:

Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.

File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Place a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus.

Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348-5069	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the credit reporting agencies without your consent. There may be fees for placing, lifting or removing a security freeze, which generally range from \$5-\$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each credit reporting agency individually.* For more information on security freezes, you may contact the three national credit reporting agencies or the FTC as described above. Since the instructions for establishing a security freeze differ from state to state, please contact the three national credit reporting agencies for more information.

The credit reporting agencies may require proper identification prior to honoring your request to place a security freeze on your credit file. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Proof of your current residential address (such as a current utility bill)
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)

For Maryland and North Carolina Residents. You can obtain information from the Maryland and North Carolina Attorney General's Offices about preventing identity theft. You may contact these offices at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (toll-free in North Carolina)
919-716-6400
www.ncdoj.gov