



METROPOLITAN HOSPITAL CENTER

1901 FIRST AVENUE, NEW YORK, NY 10029

Anthony Rajkumar
Executive Director

<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

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

Re: Notification Regarding Your Personal Health Information

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

The New York City Health and Hospitals Corporation (HHC), which operates the Metropolitan Hospital Center (Metropolitan), values the importance of protecting the confidentiality of our patients' medical records. Therefore, we regret to inform you of an incident that resulted in the possible unauthorized disclosure of your protected health information (PHI), including such information as your name, medical record number, medical diagnosis, physician's name, and limited sensitive medical information. Although we have no evidence that your PHI was inappropriately used, we are required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to inform you of this incident in writing. We also want to assist you by providing you with the steps that you can take to protect yourself from any harm that may result from this incident.

DESCRIPTION OF INCIDENT:

By way of background, HHC has implemented an information governance and security program that, among other things, monitors and detects all email communications that contain PHI and other confidential information that are sent outside of HHC's information systems without proper authorization. The incident in question, which occurred on January 15, 2015, was discovered on March 31, 2015 when, in the course of HHC's monitoring of outgoing emails, we identified an email that contained PHI, including yours, which a Metropolitan employee improperly sent from his HHC email account to his personal email account.

While there is no indication that the employee improperly used the information contained in the email, its transmission was unauthorized and certainly not condoned by Metropolitan. Therefore, in an abundance of caution, we are notifying you of this incident and advising you of the actions that we have taken and the ones that we recommend you consider taking to protect yourself from any possible adverse effects that could arise as a result of this incident.

WHAT WE HAVE DONE IN RESPONSE TO THE BREACH:

Metropolitan has promptly taken a number of steps in response to this incident. First, we interviewed the responsible Metropolitan employee and examined his HHC email account to ensure that we identified all the sites to which the email and spreadsheets were sent. We also reviewed the employee's personal email account, and were present to ensure that the employee deleted the email and spreadsheets from his personal email account.

Second, to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide **identity theft protection 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 theft protection services include Credit Monitoring and Identity Theft Consultation and Restoration. Additional information describing your services is included with this letter.

Visit kroll.idMonitoringService.com and follow the online instructions to take advantage of your Identity Theft Protection Services.

Membership Number: <<Member ID>>

kroll.idMonitoringService.com is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. To receive credit services by mail instead of online, please call 1-855-366-0145.

930U03-0615

WHAT SHOULD YOU DO IF YOU HAVE ANY QUESTIONS OR FEEL YOU HAVE AN IDENTITY THEFT ISSUE?

Call 1-855-366-0145, 8 a.m. to 5 p.m. (Central Time), Monday through Friday. Kroll's licensed investigators are standing by to answer your questions or help you with concerns you may have. *Please have your membership number ready.*

Third, we have taken steps to ensure the confidentiality and security of communications containing PHI. We have notified employees as to the importance of protecting patient information and have scheduled additional training for our staff. We have also instituted the automatic blocking of email communications containing PHI and other confidential information from being sent from HHC's information systems to any site or entity outside of the HHC security network unless for a legitimate business purpose.

Fourth, the Metropolitan employee responsible for this improper transmission has been terminated from his position by HHC.

WHAT YOU CAN DO:

In addition to enrolling in credit monitoring services, below are some additional steps you may wish to take to protect yourself from potential harm that may arise from this incident:

1) Order a free credit report. Under the federal Fair Credit Reporting Act, you are entitled to receive a free copy of your credit report from each of the three national consumer reporting companies (Equifax, Experian and TransUnion) once every twelve months. After you receive your credit report you should review it to see if it contains activity that you do not recognize, such as accounts that you have not opened, or debts that you did not incur. If you discover information in your credit report that you believe to be fraudulent, contact the credit reporting company to remove this information. You may obtain your free credit report online at www.annualcreditreport.com or by telephone at 1-877-322-8228.

Although you may request credit reports from all three credit reporting companies at the same time, another strategy would be to order from one company immediately and from the other two over a period of weeks or months to see if any unrecognized activity appears over time.

2) Place a credit alert on your consumer credit files. Call the toll-free number of any one of the three major credit reporting companies listed below to place a free 90-day fraud alert on your credit report. This can help prevent an identity thief from opening accounts in your name. As soon as the credit reporting company confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report.

Equifax: 1-800-525-6285/ www.equifax.com/ P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742) / www.experian.com / P.O. Box 9532, Allen TX 75013.

TransUnion: 1-800-680-7289 / www.transunion.com / Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

3) Monitor your account activities. Read your health insurance statements of services promptly upon receiving them to confirm that they are accurate. Also, make sure that any health care bills that you receive are accurate. Be concerned if you receive statements for medical services you did not receive. If you believe you are a victim of medical identity theft, you may make a report to the New York City Police Department at your local precinct or by calling 311.

4) Request access to your medical record and, if appropriate, file a request to amend your record. You may wish to review your medical record to determine whether your information has been compromised. Depending on your review, you may file a request to amend your record to correct any information that you believe does not appropriately apply to your medical record.

To review, copy or make changes to your medical record, please contact the Metropolitan Privacy Officer, Christopher Roberson, or the HHC Corporate Privacy and Security Officer, William Gurin, at the phone numbers provided below.

You will also find additional useful information about these and other measures you may take to protect yourself against identity theft on the following websites:

Federal Trade Commission

<http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/compromised.html>

Office of the New York Attorney General

<http://www.ag.ny.gov/consumer-frauds-bureau/identity-theft>

New York City Police Department

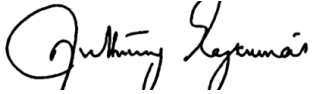
http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/Identity_Theft.pdf

OUR APOLOGY

We at Metropolitan take our role of safeguarding your personal information and using it in an appropriate manner very seriously. Metropolitan apologizes for the concern this incident may have caused and assures you that we are doing everything we can to prevent an incident of this nature from recurring.

For any questions you may have concerning this incident you may contact E. Christopher Roberson, Director of Network Privacy for the South Manhattan Healthcare Network, at (646) 672-3172, or William Gurin, Corporate Privacy and Security Officer, toll free, at 888-91-HIPAA (888-914-4722) or by email at CPO@nychhc.org.

Sincerely,

A handwritten signature in black ink that reads "Anthony Rajkumar". The signature is written in a cursive style with a large initial 'A'.


Anthony Rajkumar

¹ HIPAA Privacy Rule, 45 CFR § 164.401 et seq. "HIPAA" stands for the Health Insurance Portability and Accountability Act of 1996, which was amended by the American Recovery and Reinvestment Act of 2009. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs.

Take Advantage of Your Identity Theft Protection Services

You've been provided with access to services from Kroll, a global leader in risk mitigation. Over the past 14 years, Kroll has provided data breach response services for cases impacting more than 100 million individuals including personal consultation to more than 180,000 consumers and worked some 8,000 confirmed identity theft cases. When you need assistance, rest assured that your services are backed by an expert team who can answer any question you may have.

The following services are included in your **Credit Monitoring** package:

	<p>Kroll employs a team of experienced licensed investigators to provide you with expert, one-on-one assistance:</p> <p>Consultation: You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes best practice tips to assist in ongoing protection, 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.</p> <p>Restoration: Kroll's restoration services are the most comprehensive of any provider. Should you become a victim of identity theft, a dedicated licensed investigator can work on your behalf to resolve related issues. The investigator does more than shoulder the bulk of the recovery; they can dig deep to uncover all aspects of the theft, and then work with creditors, collection agencies, utilities, government entities, and more ... to resolve it.</p>
	<p>Credit Monitoring: Credit monitoring can be a key tool in detecting early warning signs of identity theft. You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll investigator, who can help you determine if it's an indicator of identity theft. You'll also receive "no activity" notices if there have been no changes to your data.</p>

How to Take Advantage of Your Identity Theft Protection Services

<p>Visit kroll.idMonitoringService.com and follow the online instructions to take advantage of your identity theft protection services.</p> <p>You can view your services at any time by logging onto Kroll's identity protection website. When you enroll, be prepared to provide the membership number included with the accompanying letter.</p>	<p>Help is only a phone call away.</p> <p>If you have a question, need assistance, or feel you may be a victim of identity theft, call Kroll at the toll-free number provided in the accompanying letter, and ask to speak with an investigator.</p> <p>Take advantage of this no-cost opportunity and let the experts at Kroll help you assess your situation and safeguard your identity.</p>
---	--

Kroll.idMonitoringService.com is compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox or Safari.

State Notification Requirements

All States.

You may obtain a copy of your credit report or request information on how to place a fraud alert or security freeze by contacting any of the national credit bureaus below. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Equifax P.O. Box 740241 Atlanta, GA 30374 1-800-685-1111 www.equifax.com	Experian P.O. Box 2104 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 2000 Chester, PA 19022 1-800-888-4213 www.transunion.com
---	---	---

For residents of Massachusetts.

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Massachusetts and West Virginia.

You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address,

and the date of issue. The consumer reporting agency may charge a fee of up to \$5.00 to place a freeze or lift or remove a freeze and free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

For residents of Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, and West Virginia.

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

For residents of Iowa.

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon.

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Illinois, Maryland and North Carolina.

You can obtain information from the Federal Trade Commission, and for residents of Maryland and North Carolina, from your respective state Office of the Attorney General, about steps you can take toward preventing identity theft.

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

**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 Office of
the Attorney General**
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com