



# METROPOLITAN HOSPITAL CENTER

1901 FIRST AVENUE, NEW YORK, NY 10029

Anthony Rajkumar  
Executive Director

May 18, 2015

John Q. Public  
123 Wherever Street  
Brooklyn, N.Y. 11201

Re: Notification Regarding Your Personal Health Information

Dear Patient,

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)<sup>1</sup> 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.

---

<sup>1</sup> 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.

## **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.

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 is no longer working at Metropolitan and has been terminated by HHC.

## **WHAT YOU CAN DO:**

In addition to contacting the number provided above to obtain 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](http://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/](http://www.equifax.com/) P.O. Box 740241, Atlanta, GA 30374-0241

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

- TransUnion: 1-800-680-7289 / [www.transunion.com/](http://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](http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/Identity_Theft.pdf)

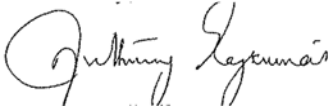
## **OUR APOLOGY**

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](mailto: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