NEW YORK CITY HEALTH & HOSPITALS CORPORATION
North Bronx Healthcare Network

JACOBI MEDICAL CENTER

NC BH NORTH CENTRAL BRONX HOSPITAL

C/O ID Experts
PO Box 6336
Portland, OR 97228-6336

WILLIAM P. WALSH
Senior Vice President

<<First Name>><<Last Name>>
<<Street Address>>
<<City>><<State>><<Zip>>

<<Date>>

Re: Notification Regarding Your Personal Health Information

Dear <<First Name>><<Last Name>>:

The New York City Health and Hospitals Corporation ("HHC"), which operates the Jacobi Medical Center ("JMC") and North Central Bronx Hospital ("NCB"), 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 unauthorized disclosure of your protected health information ("PHI"), including such information as your name, address, date of birth, telephone number, medical record number, treatment dates and types of services, limited sensitive health information, and your health insurance identification number, which may include your social security number. 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")[1] to inform you of this incident in writing and we also want to assist you by providing you with steps to take to protect yourself from any potential harm that may result from this incident.

Description of the 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 February 19, 2015, was discovered on February 27, 2015 when, in the course of HHC's monitoring of outgoing emails, we identified a number of emails containing files of PHI that were accessed by a former Jacobi employee after her employment ended on February 13, 2015. The former employee sent these files to her personal email account. She also sent these files to the email account of her new employer, which is a New York City agency that works closely with HHC. According to the former employee, she accessed and sent the subject files to these email accounts in the event that in the future she had to respond to questions about her past work at JMC.

While there is no indication that the former employer improperly used the information in these files, or that her new employer, an agency of the City of New York, has accessed, viewed or used these files, her access to and forwarding of your PHI was certainly improper and not condoned by JMC and NCB. Therefore, in an abundance of caution, we are notifying you of this incident and advising you of the actions we have taken and the ones that we recommend that you take to protect yourself from any possible adverse effects from this improper access to your PHI.

[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.

What We Have Done in Response to This Incident

JMC has promptly taken a number of steps in response to this incident. First, upon discovery of the unauthorized access of your PHI, we interviewed the former employee, who informed us that the information she accessed was not further disseminated and was subsequently deleted from her personal computer and personal e-mail account. We later conducted a forensic review of her personal computer and confirmed that the information was in fact deleted and had not been forwarded further from that computer. Additionally, the City agency, where the former employee now works, has advised us that they examined their information and email systems, as well as the computer they assigned to the former JMC employee, and they advised HHC that, after a diligent search, the subject files were not present on their systems or computer devices.

Second, we have arranged for the availability of credit monitoring services through a third party vendor, ID Experts, at no cost to you. ID Experts will provide you with their FraudStop™ Credit Edition, which includes 12 months of credit monitoring, a $20,000 insurance reimbursement policy, exclusive educational materials and complete access to their fraud resolution representatives. With this protection, ID Experts will help you resolve issues if your identity is compromised as a result of this incident. To receive these free services, however, you must contact ID Experts and enroll into the same by calling 1-866-487-6522 or going to www.myidcare.com/healthprotect. ID Experts is available Monday through Friday from 9 a.m. - 9 p.m. Eastern Standard Time. Please note that, the deadline to enroll is July 28, 2015. Attached is additional information about the services being offered by ID Experts.

You will need to reference the following access code when calling or enrolling on the website, so please do not discard this letter. ***Your Access Code: <<ID Experts will insert>>.***

Lastly, as a result of this incident, we have taken additional steps to ensure the confidentiality and security of communications containing PHI and to prevent former employees from gaining access to JMC and NCB information systems once their employment has ceased. 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.

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 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 North Bronx Healthcare Network Privacy Officer, Vincent Stanco, or the HHC Corporate Privacy and Security Officer, William Gurin, at the numbers provided below.

5) ***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 JMC take our role of safeguarding your personal information and using it in an appropriate manner very seriously. JMC 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. Please be advised that the person who accessed your information no longer has access to any of HHC's information systems, including JMC.

If you have any questions about this incident, please contact our representatives at 1-866-487-6522 between 9:00 a.m. and 9:00 p.m. (EST), Monday through Friday or go online to www.myidcare.com/healthprotect.

Very truly yours,

William P. Walsh