Bellevue Hospital Center
South Manhattan Healthcare Network

First Ave & 27th St. New York. NY 10016

April 28, 2015

Re: Notification Regarding Your Personal Health Information

Dear Mr. Patient,

The New York City Health and Hospitals Corporation ("HHC"), which operates the Bellevue Hospital Center ("Bellevue"), 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, medical record number, telephone number, e-mail address, the name of your medical insurance carrier, and limited sensitive 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")[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 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 occurred on January 15, 2015 and was discovered on February 27, 2015 when, in the course of HHC's monitoring of outgoing emails, we identified an email attachment that a Bellevue employee improperly sent to her relative's e-mail account at the relative's place of employment. The e-mail attachment contained a spreadsheet that included your PHI, as well as the PHI of other patients. According to the employee, she sent the spreadsheet to her relative for technical assistance in manipulating the spreadsheet data for Bellevue work purposes. Regardless of the employee's motivation for sending the email and attachment, the transmission of this information to an unauthorized recipient was certainly improper and is not condoned by Bellevue.

[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 of2009. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security ofhealthcare information and help the healthcare industry control administrative costs.

While there is no indication that the information on the spreadsheets, including yours, was ever improperly used, its access and viewing by an unauthorized recipient was certainly improper. 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 suggest you consider taking.

What We Have Done In Response to the Breach

Upon discovery of this incident, Bellevue has promptly taken a number of steps in response to this incident. First, we interviewed the Bellevue employee and her relative, both of whom informed us that the spreadsheet was not further forwarded to any other unauthorized recipient. Bellevue's forensic review of its employee's computer systems confirm that she did not send the spreadsheet to any other person beyond her relative.

Additionally, we obtained an affidavit from the relative wherein he states that he had deleted the spreadsheet from his work email and computer. The relative also affirmed under oath that he had requested that his employer's information technology department delete the improperly sent email and attachments from its computer systems. In summary, affidavits from the relative and from the IT department administering the relative's server attest, under oath, that the information was deleted from all sites.

Further, as a result of this incident, we have taken several steps to ensure the confidentiality and security of communications containing PHI. We have notified employees as to the importance of protecting this information and have planned 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.

Please be advised that the Bellevue employee responsible for this improper transmission is now facing disciplinary action for her transmission of PHI to an unauthorized recipient.

What You Can Do

Below are several steps you may wish to take to protect yourself from potential harm arising from this incident:

1) *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.

2) *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 Bellevue Privacy Officer, Christopher Roberson, or the HHC Corporate Privacy and Security Officer, William Gurin, at the numbers provided below

3) 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-
btlp://ww .ag.ny.gov/c n urn r-fr uds-bureau/idenLiLy-lh fl.

New York City Police Department --
hllp://www.nyc.gov/html/nvpd/downloads/pdf/crim prevention/Identity Theft.pclf

Our Apology

We at Bellevue take our role of safeguarding your personal information and using it in an appropriate manner very seriously. Bellevue 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 212-562-4316, 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

Steven R. Alexander
Executive Director
Bellevue Hospital Center