NEW YORK CITY HEALTH AND HOSPITALS CORPORATION

John P. Graham
Director, Corporate Office of HIPAA
Privacy & Security Compliance
Information Technology Services

November 30, 2010

Personal and Confidential

<Full Name>
<Street Address>
<City, State, Zip Code>

Re: Notification Regarding Your
Personal Health Information

Dear Patient:

The New York City Health and Hospitals Corporation ("HHC"), which operates Kings County Hospital Center ("Kings County"), values the importance of protecting the confidentiality of our patients' medical records. Therefore, we regret to inform you of an incident at Kings County that may have resulted in the unauthorized acquisition of some of your protected health information (PHI). This incident, which appears to have taken place on August 22, 2010, involved a cable-secured computer that was removed from a locked office at Kings County. Unfortunately, after personnel interviews and forensic analysis were conducted, we discovered on or about October 1, 2010, that the hard drive of this computer may have contained some of your PHI, specifically demographic and clinical information, such as your name, medical record number, diagnosis and treatment.

Please note that HHC has no knowledge that your health information has, in fact, been improperly accessed or disclosed. Furthermore, we do not believe that the thief's objective was to access data on the computer. This computer was brand new and was not utilized by Kings County as a data repository. The information containing your PHI consisted of random files unintentionally uploaded to this computer as part of the information system's network user profile. Nevertheless, we are required by federal regulation to make you aware of the incident and to inform you of steps you may take to protect yourself from possible harm arising from this information breach.*

Among the steps you may wish to take to protect yourself from possible adverse consequences of this incident:

*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.

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 block this information.

You may obtain your free credit report online at www.annualcreditreport.com, by telephone at 1-877-322-8228, or by completing the enclosed form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

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 financial account statements and health insurance statements of services promptly upon receiving them to confirm that they are accurate. Also, make sure that you are receiving your regular bills and that your accounts have not been switched. Be concerned if you receive credit cards that you did not apply for, or you receive communications from creditors regarding goods or services you did not purchase.

If you believe you are a victim of identity theft, you may report it 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 your medical record, please file a HIPAA Request to Access form (HHC 2426) with Health Information Management (HIM) at Kings County. After your review, if you want to make an amendment, file a HIPAA Request for Amendment form (HHC 2415) with HIM.

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

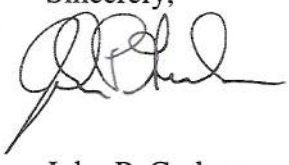
Office of the New York Attorney General –
http://www.ag.ny.gov/bureaus/consumer_frauds/tips/id_theft_victim.html

New York City Police Department --
http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/Identity_Theft.pdf

We at HHC take our role of safeguarding your personal information and using it in an appropriate manner very seriously. HHC apologizes for the concern this incident may cause you and assures you that we have taken steps to ensure that a similar breach of PHI does not recur. HHC security policies already prohibit the intentional downloading of PHI to desktop computers, but Kings County is currently adopting a new system that will encrypt information that is unintentionally downloaded as part of the computer user's profile.

You may contact Annette Griffith, the Kings County HIPAA Privacy Officer, by telephone at (718) 245-4219 regarding any questions you may have or to learn additional information concerning this breach, or you may contact me regarding this incident, toll free, at 888-91-HIPAA (888-914-4722), or by email at CPSO@nychhc.org.

Sincerely,



John P. Graham

Encl.