NEW YORK CITY HEALTH AND HOSPITALS CORPORATION

John P. Graham
Director, Oficina Corporativa de Cumplimiento de la Privacidad y la Seguridad del HIPAA
Servicios de Tecnología de la Información

30 de noviembre de 2010

Personal y confidencial

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

Asunto: Aviso sobre su información personal de salud.

Estimado/a paciente:

New York City Health and Hospitals Corporation ("HHC"), a cargo de Kings County Hospital Center ("Kings County"), valora la importancia de proteger la confidencialidad de las historias clínicas de los pacientes. Por lo tanto, lamentamos informarle de un incidente sucedido en Kings County que pudo haber ocasionado la obtención no autorizada de cierta información protegida de salud (PHI, por sus siglas en inglés). En este incidente, que aparentemente ocurrió el 22 de agosto de 2010, estuvo involucrada una computadora con cable asegurado que se extrajo de la oficina con llave del Kings County. Lamentablemente, después de entrevistas al personal y de haber realizado los análisis delictivos, el 1 de octubre de 2010, o alrededor de esa fecha, descubrimos que el disco duro de dicha computadora puede haber tenido una parte de su PHI, en especial, información clínica y demográfica, tal como nombre, número de historia clínica, diagnósticos y tratamientos.

Tenga en cuenta que HHC no tiene conocimiento de que alguien efectivamente haya tenido acceso indebido a su información de salud o que ésta haya sido indebidamente divulgada. Además, no creemos que el objetivo del ladrón sea acceder a los datos de la computadora. Esta computadora era nueva y el Kings County no la utilizaba como un repositorio de datos. La información que contenía su PHI eran archivos al azar que se habían cargado involuntariamente a esta información como parte del perfil de usuario de la red del sistema de información. Sin embargo, estamos obligados en virtud de la legislación federal de informarle del incidente y de informarle de las medidas que usted puede tomar frente a posibles daños derivados de esta violación de información.*

*Norma de privacidad HIPAA, 45 CFR § 164.401 *y siguientes* "HIPAA" es la sigla que corresponde a la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (Health Insurance Portability and Accountability Act) de 1996, que fue modificada por la Ley de Recuperación y Reinversión de los Estados Unidos (American Recovery and Reinvestment Act) de 2009.

A continuación se incluyen algunas medidas que quizá quiera tomar para protegerse de las posibles consecuencias adversas de este incidente:

1) *Pedir un informe gratuito de crédito.* Bajo la Ley federal de Informe Imparcial de Crédito, cada doce meses usted tiene derecho a recibir una copia gratuita de su informe de crédito de cada una de las tres empresas nacionales de informes de crédito (Equifax, Experian y TransUnion). Después de recibir su informe de crédito, deberá revisarlo para ver si contiene alguna actividad que usted no reconozca, como cuentas que usted no haya abierto o deudas que no haya contraído. Si descubre algún dato en su informe de crédito que usted considera que obedece a alguna operación fraudulenta, comuníquese con la empresa de informes de crédito para bloquear esta información.

Usted puede obtener su informe gratuito de crédito por Internet en www.annualcreditreport.com, por teléfono, llamando al 1-877-322-8228, o puede completar el formulario adjunto y enviarlo por correo a Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Si bien usted puede solicitar informes de crédito a las tres empresas de informes de crédito al mismo tiempo, otra alternativa sería realizar la solicitud a una de las empresas inmediatamente y a las otras dos después de dejar pasar un período de semanas o meses, para ver si con el tiempo aparece alguna actividad adicional, no reconocida.

2) *Colocar una alerta de crédito en sus archivos de crédito del consumidor.* Llame al número gratuito de cualquiera de las tres principales empresas de informes de crédito que figuran debajo para colocar una alerta de fraude gratuita durante 90 días en su informe de crédito. Esta medida puede ayudar a evitar que un ladrón de identidad abra cuentas a su nombre. Tan pronto como la empresa de informes de crédito confirma su alerta de fraude, se notificará automáticamente a las otras dos agencias de informes para que coloquen alertas en su informe de crédito.

- **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) *Controlar las actividades de su cuenta.* Lea sus resúmenes de estados financieros y resúmenes de prestaciones del seguro médico tan pronto los reciba para asegurarse de que sean correctos. Además, asegúrese de seguir recibiendo sus facturas habituales y que no se hayan modificado sus cuentas. Esté alerta si recibe tarjetas de crédito que usted no solicitó o si recibe alguna comunicación de acreedores por bienes o servicios que usted no adquirió.
Si considera que ha sido víctima de un robo de identidad, puede informar al Departamento de Policía de la Ciudad de Nueva York, a la comisaría local o llamar al 311.

4) *Solicitar el acceso a su historia clínica y, si corresponde, presentar una solicitud para modificar su historia.* Quizá desee revisar su historia clínica para determinar si sus datos

se han visto comprometidos. Según el resultado de su revisión, puede presentar un pedido para modificar su historia clínica y corregir toda información que considera que no corresponde con su historia clínica.

Para revisar su historia clínica, presente un formulario de Solicitud de Acceso HIPAA (HHC 2426) ante la Administración de Datos de Salud (HIM) del Kings County. Después de revisar la historia clínica, si desea introducir cambios, presente un formulario de Solicitud de Modificación HIPAA (HHC 2415) ante la HIM.

5) *También encontrará información adicional de utilidad* sobre éstas y otras medidas que usted puede tomar para protegerse contra el robo de identidad en los siguientes sitios web:

Comisión Federal de Comercio (Federal Trade Commission)
http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/compromised.html

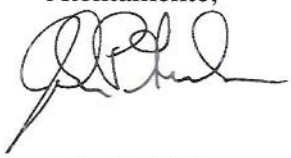
Oficina de la Fiscalía General de Nueva York (Office of the New York Attorney General)
http://www.ag.ny.gov/bureaus/consumer_frauds/tips/id_theft_victim.html

Departamento de Policía de la Ciudad de Nueva York (New York City Police Department)
http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/Identity_Theft.pdf

En HHC nos tomamos muy en serio nuestra tarea de proteger sus datos personales y usarlos en forma adecuada. HHC lamenta la preocupación que este incidente puede causarle y le asegura que se han tomado medidas para garantizar que no se vuelva a repetir una violación similar de PHI. Las políticas de seguridad de HHC prohíben la descarga intencional de PHI a computadoras de escritorio, pero actualmente el Kings County está adoptando un nuevo sistema que encriptará aquella información que se descarga involuntariamente como parte del perfil del usuario de la computadora.

Puede comunicarse con Annette Griffith, encargada de privacidad de HIPAA del Kings County, por teléfono al (718) 245-4219 si tiene alguna pregunta o necesita información adicional con relación a esta violación, o puede comunicarse conmigo por este incidente llamando en forma gratuita al 888-91-HIPAA (888-914-4722), o por correo electrónico al CPSO@nychhc.org.

Atentamente,



John P. Graham

Adjuntos