Bayamón Medical Center

Puerto Rico Women's and Children's Hospital

19 de julio de 2019

Estimado(a):

Le escribo a nombre de Bayamón Medical Center y Puerto Rico Women and Children's Hospital (colectivamente, los "Hospitales") para informarle de un incidente que afectó la red informática de los Hospitales. La protección de su información personal es muy importante para nosotros, por lo que inmediatamente adoptamos medidas para abordar la situación.

¿Qué ocurrió?
El 21 de mayo de 2019, obtuvimos conocimiento que su información estuvo envuelta en un incidente de bloqueo externo que afectó la red informática de los Hospitales. El tipo de información bloqueada, y a la cual los Hospitales no tuvieron acceso por un período corto de tiempo, incluyó información clínica, demográfica y financiera tales como su nombre completo, y en algunos casos su número de seguro social, su fecha de nacimiento y su diagnóstico. Inmediatamente tomamos medidas para garantizar la seguridad de su información. Ninguno de sus datos se perdió como resultado del incidente, y hasta la fecha no hay evidencia que sugiera que su información fue extraída de nuestra red o que ha habido algún intento de hacer uso indebido de su información.

¿Qué estamos haciendo?
Estamos manejando este incidente con la mayor seriedad y diligencia ya que la seguridad de su información es vital para nosotros. Poco después de enterarnos del incidente, comenzamos una investigación interna y contratamos a un consultor externo para que nos ayudara a descifrar y recuperar la información de nuestros pacientes. Como resultado de nuestra investigación, los Hospitales y sus consultores entienden que la información de nuestros pacientes fue simplemente encriptada (bloqueada) y actualmente no hay indicios de que la información en sí haya sido utilizada por una persona no autorizada. Continuaremos monitoreando la situación y le contactaremos si sugiriese alguna novedad. También estamos reforzando nuestros protocolos de seguridad y brindando capacitación adicional a nuestros empleados para reducir la probabilidad de que ocurra un evento similar en el futuro.

¿Qué puede hacer usted?
Aunque le hemos indicado que no obtuvimos evidencia alguna que sugiera que su información ha sido utilizada por una persona no autorizada como resultado del incidente, incluimos el documento Pasos Recomendados para Proteger su Información con información sobre los pasos adicionales que puede seguir en caso de estimarlo necesario.

Somos muy conscientes de lo importante que es para nuestros pacientes su información personal y nos disculpamos por cualquier inconveniente que este incidente pueda haber causado. En nuestros Hospitales estamos comprometidos a brindar atención de calidad, incluyendo la protección de la información personal de nuestros

pacientes. Si tiene alguna pregunta con respecto a este aviso, se puede comunicar con nosotros al (855) 493-7267 y provea el número de compromiso DB13632.

Atentamente,

José S. Rosado
Director Ejecutivo
Bayamón Medical Center
Puerto Rico Women and Children's Hospital

Pasos Recomendados para Proteger su Información

1. Teléfono. Contáctenos al (855) 493-7267 para obtener información adicional sobre este incidente y hable con representantes conocedores sobre los pasos apropiados para proteger su identidad crediticia. Tenga a la mano el número de compromiso DB13632.

2. Revise sus informes de crédito. Como medida de precaución le recomendamos que permanezca atento revisando sus estados de cuenta e informes de crédito. Bajo la ley federal usted tiene derecho a obtener una copia gratuita de su informe de crédito cada 12 meses de cada una de las tres principales compañías de informe de crédito. Para obtener un informe de crédito anual gratuito, visite www.annualcreditreport.com o llame al 1-877-322-8228. Es posible que desee escalonar sus solicitudes para que reciba un informe gratuito de una de las tres agencias de crédito cada cuatro meses.

También debe saber que tiene derecho a presentar un informe policial si alguna vez experimenta fraude de identidad. Tenga en cuenta que, con el fin de presentar un informe de delito o de incidente de robo de identidad, es probable que tenga que proporcionar algún tipo de prueba que demuestre que usted ha sido una víctima. A menudo se requiere un informe policial para disputar actos fraudulentos. Usted puede reportar presuntos incidentes de robo de identidad a las autoridades locales de la ley o al Procurador General de los Estados Unidos.

3. Establezca alertas de fraude con las tres agencias de crédito. Puede colocar una alerta de fraude en una de las tres agencias de crédito principales por teléfono y también a través del sitio web de Experian o Equifax. Una alerta de fraude le indica a los acreedores que sigan ciertos procedimientos, incluido el contacto con usted, antes de que abran cuentas nuevas o cambien sus cuentas existentes. Por esta razón, colocar una alerta de fraude puede protegerle, pero también puede retrasarle cuando usted solicite crédito. La información de contacto de las tres agencias es la siguiente:

Agencias Nacionales de Informe de Crédito

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box I 05069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	www.transunion.com

Solo es necesario ponerse en contacto con UNA de estas agencias de crédito y utilizar solo UNO de estos métodos. Tan pronto como una de las tres agencias confirma su alerta de fraude, las demás son notificadas para colocar alertas en sus registros. Usted recibirá cartas de confirmación vía correo y entonces podrá solicitar los tres informes de crédito de forma gratuita para su revisión. Una alerta inicial de fraude durante un año.

A CONSIDERAR: **No se le permite a nadie colocar una alerta de fraude en su informe de crédito, excepto a usted.**

4. Congelación de seguridad. Al colocar una congelación de seguridad, alguien que adquiera fraudulentamente su información de identificación personal no podrá usar esa información para abrir cuentas nuevas o pedir dinero prestado en su nombre. Deberá ponerse en contacto con las tres agencias nacionales de informes de crédito mencionadas anteriormente para colocar la congelación. Tenga en cuenta que cuando usted coloca la congelación, usted no será capaz de pedir dinero prestado, obtener crédito instantáneo, u obtener una nueva tarjeta de crédito basta que usted elimine temporalmente o retire permanentemente la congelación. No hay ningún costo para congelar o descongelar su expediente de crédito.

5. **Información adicional.** Puede obtener información adicional sobre los pasos que puede seguir para evitar el robo de identidad de la Comisión Federal de Comercio (Federal Trade Commission o FTC, por sus siglas en inglés) quien también alienta a aquellos que descubren que su información ha sido utilizada indebidamente a presentar una querella con ellos.

Todos los Residentes de los Estados Unidos: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.