

Aviso de filtración de datos

Recientemente, la ciudad de Filadelfia (la "Ciudad") experimentó una filtración de datos que impactaría en la seguridad de la información de algunos pacientes que se atienden en los Centros de Salud de la ciudad y el Laboratorio de Salud Pública a cargo del Departamento de Salud Pública.

¿Qué ocurrió? El 28 de mayo de 2020, la Ciudad detectó actividades sospechosas relacionadas con la cuenta de correo electrónico de un empleado del Departamento de Salud Pública. La Ciudad inició, rápidamente, una investigación interna para determinar la naturaleza y el alcance de la actividad, y también la magnitud de la información que pudo verse afectada. La investigación inicial de la Ciudad confirmó que la cuenta de correo electrónico sufrió un acceso no autorizado el 28 de mayo de 2020. A medida que se profundizó la investigación, la Ciudad confirmó que otras cuentas de correo electrónico de empleados del Departamento de Salud sufrieron accesos no autorizados de manera intermitente entre el 28 de mayo y el 20 de julio de 2020. Con la ayuda de especialistas en informática forense, la Ciudad está revisando detalladamente las cuentas de correo electrónico afectadas para confirmar el alcance de los accesos no autorizados para determinar si las cuentas contaban con información confidencial y para identificar a las personas cuya información pudo verse afectada. Luego de completar esta revisión, la Ciudad trabajará rápidamente para enviar un aviso por escrito de este suceso a las personas afectadas y para proporcionar recursos de protección de identidad que puedan ayudarlos.

¿Qué tipo de información estaba involucrada? La investigación de la Ciudad sobre este suceso está en curso y el alcance de la información comprometida todavía no se determinó. Sin embargo, a la fecha, la investigación de la Ciudad sugiere que el incidente lo causó una campaña de fraude cibernético (phishing) que se originó en otro departamento de la Ciudad y en la que se vieron afectadas múltiples cuentas de correo electrónico de varios empleados de distintos departamentos de la Ciudad. La Ciudad sospecha que algunas de las cuentas de correo electrónico afectadas contienen información personal, incluso información protegida de salud como nombres, fechas de nacimiento, direcciones, números de cuentas o de historias clínicas, información del seguro médico e información clínica. Tras completar la revisión, la Ciudad proporcionará los detalles adicionales a las personas afectadas.

¿Qué está haciendo la Ciudad? La privacidad de las personas a las que atendemos es muy importante para nosotros y continuaremos haciendo todo lo posible por protegerla. Apenas fuimos notificados de este suceso, actuamos rápidamente para confirmar y para mejorar la seguridad de nuestros sistemas. Esto incluyó resetear las contraseñas de las cuentas de correo electrónico de los empleados que se vieron afectadas, incrementar el monitoreo de la actividad de la red e implementar herramientas para mejorar la seguridad de los correos electrónicos. Como se describió más arriba, también iniciamos una investigación profunda con la ayuda de especialistas externos en informática forense para determinar completamente la naturaleza y el alcance de este incidente. Como parte de nuestro compromiso con la privacidad y la seguridad, estamos revisando nuestras políticas y procedimientos actuales para identificar una mejor manera de prevenir incidentes como este en el futuro.

¿Qué puede hacer usted? Puede obtener más información sobre cómo protegerse contra el posible uso indebido de la información en las *Políticas de Protección de Privacidad a continuación*.

Para obtener más información. Entendemos que debe tener muchas preguntas sobre este incidente que quedaron sin responder en este aviso. Mientras nuestra investigación siga en curso, llame a nuestra línea gratuita al 1-888-714-2840 *si tiene más preguntas*.

Políticas de Protección de Privacidad

Monitoreo de cuentas

La Ciudad recomienda a las personas a estar alerta a incidentes de robo de identidad o fraude, a revisar los resúmenes de cuenta y las explicaciones de los beneficios, y a monitorear los informes de crédito para detectar actividad sospechosa. Según la legislación de los Estados Unidos, las personas mayores de dieciocho (18) años tienen derecho a recibir un informe crediticio anual gratis de cada una de las tres oficinas principales de información crediticia. Para solicitar su informe crediticio gratuito, ingrese en www.annualcreditreport.com o llame gratis al 1-877-322-8228. También puede comunicarse con las tres oficinas principales de información crediticia directamente para solicitar una copia gratuita de su informe crediticio. La información de contacto de las oficinas de información crediticia es la siguiente:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

Puede obtener más información sobre robos de identidad, alertas de fraude, congelamiento de seguridad y los pasos que puede tomar para protegerse comunicándose con las oficinas de información crediticia de los consumidores, la Comisión Federal de Comercio o la Oficina del fiscal general de Pensilvania.

La información de contacto de la Comisión Federal de Comercio es la siguiente: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. La Comisión Federal de Comercio también recomienda que aquellos que descubran que fueron víctimas del uso indebido de su información presenten una queja ante la Comisión. Puede obtener información sobre cómo presentar dicha queja comunicándose por medio de la información de contacto provista más arriba. Tiene derecho a realizar una denuncia policial si alguna vez es víctima de un robo de identidad o de un fraude. Tenga en cuenta que, para realizar una denuncia ante las autoridades por robo de identidad, usted deba, probablemente, presentar pruebas que comprueben que es una víctima. Si sospecha o sabe de un robo de identidad, también debe informarlo a las autoridades y a la fiscalía general de su estado. Este aviso no fue demorado por las autoridades.