

Aviso de incidente de privacidad de datos

Actualizado el 24 de junio de 2025

El 28 de noviembre de 2023, publicamos un aviso en este sitio para informar que Capital Health había experimentado interrupciones en su red debido a un incidente de ciberseguridad. Nuestra investigación de ese incidente ha concluido y estamos actualizando nuestro aviso anterior para proporcionar más información sobre el incidente.

¿Qué ocurrió?

Nuestra investigación determinó que una persona no autorizada accedió a algunos de nuestros sistemas del 11 de noviembre al 26 de noviembre de 2023. Lo más importante es que continuamos brindando atención a los pacientes durante toda nuestra respuesta al incidente, y todos nuestros hospitales y clínicas operaron con normalidad.

Alrededor del 1 de diciembre de 2023, la investigación forense determinó que un tercero no autorizado adquirió ciertos archivos de la red de la organización o accedió a ellos. No hemos encontrado evidencia de que información personal o información de salud protegida haya sido utilizada indebidamente a causa del incidente.

¿Qué estamos haciendo?

Tras conocer el incidente, iniciamos inmediatamente una investigación con la asistencia de una empresa externa líder en seguridad forense para determinar la naturaleza y el alcance de la actividad, y garantizar la seguridad de nuestros sistemas informáticos y de nuestra red. También reportamos el incidente a las autoridades, incluyendo al FBI y a la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA).

Luego realizamos una revisión detallada de los archivos afectados para determinar si contenían información personal o información de salud protegida, y a quién pertenecía dicha información. Este proceso requirió mucho tiempo, pero fue necesario para identificar adecuadamente a las posibles personas afectadas en la medida razonablemente posible. Identificamos a las personas cuya información personal creemos razonablemente que estuvo involucrada en el incidente y les estamos enviando un aviso por escrito a la dirección postal que tenemos registrada, de conformidad con las leyes aplicables.

Por precaución y de conformidad con la ley aplicable, estamos proporcionando este aviso para que las personas puedan tomar medidas para minimizar el riesgo de que su información sea utilizada indebidamente. Hemos incluido una breve descripción de las medidas que puede tomar para proteger su identidad, crédito e información personal.

Como medida de precaución adicional, también ofrecemos acceso gratuito a servicios de control de identidad, asesoría en casos de fraude y restauración de identidades robadas para ayudar a mitigar cualquier posible daño sin costo alguno para usted. A continuación, encontrará más información sobre la inscripción en estos servicios.

Capital Health se esfuerza por proteger la privacidad y la seguridad de la información personal y de la información de salud protegida. Hemos trabajado con diligencia para determinar cómo ocurrió este incidente y hemos tomado las medidas adecuadas para evitar una situación similar en el futuro. Desde el incidente, hemos implementado una serie de mejoras en ciberseguridad,

que incluyen, entre otras, la instalación de software adicional de detección y respuesta en los puntos finales, así como el restablecimiento de todas las contraseñas.

¿Qué información estuvo involucrada?

Con base en nuestra investigación y de manera consistente con otros incidentes de ciberseguridad que han afectado tanto al sector de la salud como a otras industrias, creemos que existe la posibilidad de que los siguientes tipos de información hayan estado involucrados en el incidente: nombres, direcciones, números de Seguro Social, fechas de nacimiento, direcciones de correo electrónico, números de teléfono y, posiblemente, información clínica

¿Qué puede hacer usted?

Como en cualquier incidente de datos, le recomendamos que se mantenga alerta y considere tomar medidas para evitar el robo de identidad, obtener información adicional y proteger su información personal. Las contraseñas comunes o aquellas que esté utilizando en varias cuentas deben actualizarse por contraseñas nuevas y complejas para mayor seguridad. A continuación, se describen más medidas.

Como se mencionó anteriormente, estamos ofreciendo acceso gratuito a servicios de control de identidad, asesoría en casos de fraude y restauración de identidades robadas para ayudar a mitigar cualquier posible daño. Alentamos a las personas potencialmente afectadas a comunicarse con IDX si tienen alguna pregunta y a inscribirse en los servicios de protección de identidad sin costo llamando al 888-906-4476. Los representantes de IDX están disponibles de lunes a viernes de 9 a. m. a 9 p. m., hora del Este.

Lamentamos sinceramente esta situación y las molestias que pueda causarle.

Medidas recomendadas para ayudarlo a proteger su información:

Le recomendamos mantenerse alerta y considerar tomar las siguientes medidas para evitar el robo de identidad, obtener información adicional y proteger su información personal:

Obtenga su informe de crédito. Solicite su reporte de crédito gratuito en www.annualcreditreport.com, llame sin costo al 877-322-8228 o complete el Formulario de solicitud de reporte de crédito anual en el sitio web de la Comisión Federal de Comercio de Estados Unidos en www.ftc.gov. Cuando reciba su reporte de crédito, revíselo detenidamente. Revise si hay alguna inexactitud o cuentas que no reconozca, y notifique a las agencias de crédito lo antes posible en caso de que las haya. Usted tiene derechos bajo la Ley de Informe Justo de Crédito ("FCRA") federal. Estos incluyen, entre otros, el derecho a saber qué información hay en su expediente; a disputar información incompleta o inexacta; y a que las agencias de informes crediticios corrijan o eliminen información inexacta, incompleta o que no pueda ser verificada.

Ponga una alerta de fraude en su expediente de crédito. Una alerta de fraude lo ayuda a protegerse contra un ladrón de identidad que intente abrir crédito nuevo a su nombre. Con esta alerta, cuando un comerciante revise su historial crediticio al solicitar crédito, recibirá un aviso de que usted podría ser víctima de robo de identidad y deberá tomar medidas para verificar su identidad. También tiene derecho a poner un "congelamiento de seguridad" en su expediente de crédito. Un congelamiento de seguridad generalmente impedirá que los acreedores accedan a su expediente crediticio en las tres agencias nacionales de crédito sin su consentimiento.

Puede poner una alerta de fraude o solicitar un congelamiento de seguridad poniéndose en contacto con las agencias de crédito. Las agencias de crédito pueden exigirle que proporcione una identificación adecuada antes de atender su solicitud.

Equifax

P.O. Box 740241

Atlanta, GA 30374

1-800-685-1111

www.equifax.com

Experian

P.O. Box 9532

Allen, TX 75013

1-888-397-3742

www.experian.com

TransUnion

P.O. Box 2000

Chester, PA 19016

1-800-916-8800

www.transunion.com

Elimine su nombre de las listas de correo de ofertas de crédito preaprobadas por aproximadamente seis meses. Si aún no lo hace, preste mucha atención a todas las facturas y los cargos en su tarjeta de crédito por artículos que no contrató ni compró. Esto incluye la explicación de las prestaciones y las declaraciones de la póliza de seguro médico. Revise con frecuencia todos los estados de cuenta de sus cuentas bancarias para detectar cheques, compras o deducciones que usted no haya realizado. Tenga en cuenta que, aunque al principio no detecte actividad sospechosa, debe continuar revisando esta información periódicamente, ya que los ladrones de identidad a veces retienen la información personal robada antes de usarla.

La Comisión Federal de Comercio ("FTC") ofrece asistencia al consumidor y material educativo relacionado con el robo de identidad, cuestiones de privacidad y cómo evitar el robo de identidad. También puede obtener información sobre las alertas de fraude y los congelamientos de seguridad a través de las agencias de informes crediticios, el fiscal general de su estado y la FTC. Si detecta cualquier incidente de robo de identidad o fraude, repórtelo inmediatamente a las autoridades policiales locales, al fiscal general de su estado o a la Comisión Federal de Comercio ("FTC"). Puede obtener más información sobre cómo protegerse contra el robo de identidad (incluido cómo colocar una alerta de fraude o un congelamiento de seguridad) comunicándose con la FTC al 1-877-IDTHEFT (1-877-438-4338) o visitando www.ftc.gov/idtheft. La dirección postal de la FTC es Federal Trade Commission, Consumer

Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580. Usted tiene derecho a obtener una copia del informe policial correspondiente relacionado con este incidente, si hubiera uno.

Para residentes del distrito de Columbia: puede obtener información adicional sobre las medidas para evitar el robo de identidad en la oficina del fiscal general del distrito de Columbia en 441 4th Street, NW, Washington, DC 20001, 202-727-3400, www.oag.dc.gov.

Para residentes de Maryland: puede obtener información sobre las medidas que puede tomar para ayudar a prevenir el robo de identidad del fiscal general de Maryland en 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.marylandattorneygeneral.gov.

Para residentes de Nuevo México: tiene derechos conforme a la Ley de Informe Justo de Crédito ("FCRA") federal. Estos incluyen, entre otros, el derecho a saber qué información hay en su expediente; a disputar información incompleta o inexacta; y a que las agencias de informes crediticios corrijan o eliminen información inexacta, incompleta o que no pueda ser verificada. Para obtener más información sobre la FCRA, visite <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act> o www.ftc.gov. Además, los consumidores de Nuevo México pueden solicitar un congelamiento de seguridad de su informe de crédito para proteger su privacidad y asegurarse de que no se otorgue crédito a su nombre sin su conocimiento. Usted puede presentar una declaración de eliminación para que se elimine la información incluida en su informe de crédito por haber sido víctima de robo de identidad. Tiene derecho a colocar un congelamiento de seguridad en su informe de crédito o a presentar una declaración de eliminación conforme a la Ley de Informe Justo de Crédito y Seguridad de Identidad. Para obtener más información sobre cómo los consumidores de Nuevo México pueden obtener un congelamiento de seguridad, visite <http://consumersunion.org/pdf/security/securityNM.pdf>.

Para residentes de Nueva York: también puede comunicarse con las siguientes agencias estatales para obtener información sobre la respuesta a violaciones de seguridad y la prevención y protección contra el robo de identidad. 1) Fiscal general de Nueva York, (212) 416-8433 o <https://ag.ny.gov>; o 2) División de Protección del Consumidor del Departamento de Estado de Nueva York, (800) 697-1220 o <https://dos.ny.gov/consumer-protection>.

Para residentes de Carolina del Norte: puede obtener información sobre las medidas que puede tomar para ayudar a prevenir el robo de identidad a través de la oficina del fiscal general de Carolina del Norte en 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

Para residentes de Rhode Island: puede ponerse en contacto con el fiscal general de su estado y obtener información de él o denunciar el robo de identidad ante él en:

Oficina del fiscal general de Rhode Island

150 South Main Street

Providence, RI 02903

Teléfono: (401) 274-4400

Sitio web: www.riag.ri.gov