Centers for Medicare & Medicaid Services
7500 Security Blvd.
Baltimore, MD 21244-1850

Nombre
Dirección

16 de diciembre de 2022

Estimado <Nombre>,

Le escribimos para informarle sobre un posible incidente de privacidad que involucra su información personal relacionada con los registros de pago de primas y derechos de Medicare. Los Centros de Servicios de Medicare y Medicaid (CMS), la agencia federal que administra el programa de Medicare, le envían esta carta para que pueda comprender más sobre este incidente, cómo lo estamos abordando y los pasos adicionales que puede tomar para proteger su privacidad. Le emitiremos una nueva tarjeta de Medicare con un nuevo número de Medicare y hemos proporcionado información con este aviso sobre los servicios gratuitos de control de crédito. Esto no afecta sus beneficios o cobertura de Medicare.

¿Qué sucedió?

El 8 de octubre de 2022, *Healthcare Management Solutions (HMS), LLC*, un subcontratista de CMS, fue objeto de un ataque de ransomware (secuestro de datos) en su red corporativa. HMS maneja los datos de CMS como parte del procesamiento de los registros de derecho y elegibilidad de Medicare, además de los pagos de primas. La información inicial indica que HMS actuó en violación de sus obligaciones con CMS, y CMS continúa investigando el incidente. No se violaron los sistemas de CMS y no hubo datos de reclamos de Medicare involucrados. El 9 de octubre de 2022, se notificó a CMS que los sistemas del subcontratista habían estado sujetos a un incidente de ciberseguridad, pero los sistemas de CMS no estaban involucrados. A medida que se dispuso de más información, el 18 de octubre de 2022, CMS determinó con gran confianza que el incidente potencialmente incluía información de identificación personal e información de salud protegida para algunos afiliados a Medicare. Desde entonces, CMS ha estado trabajando diligentemente con el contratista para determinar qué información y qué personas pueden haber sido afectadas.

¿Qué información estuvo involucrada?

Después de una cuidadosa revisión, hemos determinado que su información personal y la de Medicare pueden haberse visto comprometidas. Esta información puede haber incluido lo siguiente:

- Nombre
- Dirección
- Fecha de nacimiento
- Número de teléfono
- Número de Seguro Social
- Identificador de beneficiario de Medicare
- Información bancaria, incluidos los números de ruta y de cuenta

- Información sobre derechos, inscripción y primas de Medicare.

No hubo datos de reclamos involucrados en este incidente.

Qué estamos haciendo

Cuando se informó el incidente, comenzamos de inmediato una investigación, trabajando con el contratista y los expertos en seguridad cibernética para identificar qué información personal, si alguna, podría haberse visto comprometida. CMS continúa investigando este incidente y seguirá tomando todas las medidas apropiadas para salvaguardar la información confiada a CMS.

Lo que puede hacer

En este momento, no tenemos conocimiento de ningún informe de fraude de identidad o uso indebido de su información como resultado directo de este incidente. Sin embargo, por precaución, le estamos emitiendo una nueva tarjeta de Medicare con un nuevo número. CMS le enviará por correo la nueva tarjeta a su dirección en las próximas semanas. Mientras tanto, puede continuar usando su tarjeta de Medicare existente. Después de obtener su nueva tarjeta, debe:

1. Seguir las instrucciones en la carta que viene con su nueva tarjeta.
2. Destruir su antigua tarjeta de Medicare.
3. Informar a sus proveedores que tiene un nuevo número de Medicare.

Mientras continuamos investigando qué información bancaria, si alguna, puede haberse visto comprometida, si tiene inquietudes, comuníquese con su institución financiera e infórmeles que su información bancaria puede haberse visto comprometida. Además, puede inscribirse en el servicio gratuito de control de crédito Equifax Complete Premier. Usted **no** necesita usar su tarjeta de crédito para inscribirse en el servicio. Para activar su monitoreo de crédito gratuito:

- Por favor revise el documento adjunto con instrucciones
- Puede inscribirse en línea o llamando al xxx-xxx-xxxx
- Inscríbase antes de **31 de marzo de 2023** Su código no funcionará después de esta fecha
- Visite el sitio web de Equifax para inscribirse en: **www.xxx.com**

Si tiene preguntas sobre el servicio de control de crédito o para inscribirse en Equifax Complete Premier por teléfono, llame al equipo de atención al cliente de Equifax antes del 31 de marzo de 2023 al xxx-xxx-xxxx.

Adjuntamos información adicional sobre otros pasos que puede tomar para proteger aún más su privacidad.

Para más información

Nos tomamos muy en serio la privacidad y la seguridad de su información personal. Pedimos disculpas por las molestias que este incidente de privacidad ha causado.

Si tiene más preguntas sobre este incidente, llame a la línea de respuesta gratuita dedicada y confidencial de Equifax al xxx-xxx-xxxx. Esta línea de respuesta cuenta con profesionales familiarizados con este incidente que saben lo que puede hacer para protegerse contra el uso indebido de su información. La línea de respuesta está disponible de lunes a viernes, de 9 am a 9 pm, hora del Este. También puede llamar al 1-800-MEDICARE (1-800-633-4227) si tiene preguntas o inquietudes generales sobre Medicare.

Otros pasos para protegerse

1. Coloque una alerta de fraude en su archivo de crédito

La Comisión Federal de Comercio (FTC) recomienda que coloque una "Alerta de fraude" inicial de un año en sus archivos de crédito, sin cargo para usted. Una alerta de fraude les indica a los acreedores que se comuniquen con usted personalmente antes de abrir cuentas nuevas. Para colocar una alerta de fraude, llame a una de las tres principales agencias de crédito a los números que se indican a continuación. Tan pronto como una agencia de crédito confirme su alerta de fraude, notificará a los demás.

Equifax
P.O Box 105788
Atlanta, Georgia 30348
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion LLC
P.O. Box 6790
Fullerton, Pennsylvania 92834-6790
https://www.transunion.com/fraud-alerts
(800) 680-7289

2. Considere colocar un congelamiento de seguridad en su archivo de crédito

Si le preocupa mucho convertirse en víctima de fraude o robo de identidad, puede solicitar que se coloque un "Congelamiento de seguridad" en su archivo de crédito, sin cargo. Un congelamiento de seguridad prohíbe, con ciertas excepciones específicas, que las agencias de informes crediticios divulguen su informe de crédito o cualquier información contenida en él sin su autorización expresa. Puede colocar un congelamiento de seguridad en su informe de crédito comunicándose individualmente con las tres compañías de informes de crédito a nivel nacional a los números a continuación y siguiendo las instrucciones indicadas o enviando una solicitud por escrito, por correo, a las tres compañías de informes de crédito:

Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, Pennsylvania 19016
http://www.transunion.com/creditfreeze
1-888-909-8872

Para realizar el congelamiento de seguridad, deberá proporcionar su nombre, dirección, fecha de nacimiento, número de Seguro Social y otra información personal. Después de recibir su solicitud de congelamiento, cada compañía de informes crediticios le enviará una carta de confirmación que contiene un PIN (número de identificación personal) o contraseña única. Guarde el PIN o la contraseña en un lugar seguro. Lo necesitará si decide levantar el congelamiento.

Si su información personal ha sido utilizada para presentar una declaración de impuestos falsa, para abrir una cuenta o intentar abrir una cuenta a su nombre o para cometer fraude u otros delitos en su contra, puede presentar un informe policial en la ciudad en la que reside actualmente.

3. Obtenga un informe de crédito gratuito

Según la ley federal, usted tiene derecho a recibir un informe de crédito gratuito cada 12 meses de cada una de las tres principales empresas nacionales de informes de crédito mencionadas anteriormente. Llame al **1-877-322-8228** o solicite sus informes de crédito gratuitos en línea en **www.annualcreditreport.com**. Cuando reciba sus informes de crédito, revíselos en busca de problemas. Identifique las cuentas que no abrió o las consultas de los acreedores que no autorizó. Verifique que toda la información sea correcta. Si tiene preguntas o nota información incorrecta, comuníquese con la compañía de informes crediticios.

Incluso si no encuentra ninguna actividad sospechosa en sus informes crediticios iniciales, la FTC recomienda que revise sus informes crediticios periódicamente. Revisar su informe de crédito periódicamente puede ayudarlo a detectar problemas y solucionarlos rápidamente.

Si encuentra actividad sospechosa en sus informes crediticios o tiene razones para creer que su información está siendo utilizada de manera indebida, llame a la agencia local encargada de hacer cumplir la ley y presente un informe policial. Asegúrese de obtener una copia del informe policial, ya que muchos acreedores querrán la información que contiene para absolverlo de las deudas fraudulentas. También puede presentar una queja ante la FTC comunicándose con ellos en la web en www.ftc.gov/idtheft, por teléfono al 1-877-IDTHEFT (1-877-438-4338), o por correo a la Comisión Federal de Comercio, Centro de Respuesta al Consumidor, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Su queja se agregará a la Cámara de compensación de datos de robo de identidad de la FTC, donde estará accesible para las fuerzas del orden público para sus investigaciones. Además, puede obtener información de la FTC sobre alertas de fraude y congelamientos de seguridad.

4. Proteja su información médica

No tenemos evidencia de que su información médica involucrada en este incidente haya sido o vaya a ser utilizada para propósitos no deseados. Sin embargo, las siguientes prácticas pueden proporcionar garantías adicionales para protegerse contra el robo de identidad médica.

- Solo comparta sus tarjetas de seguro médico con sus proveedores de atención médica y otros miembros de la familia que estén cubiertos por su plan de seguro o que lo ayuden con su atención médica.
- Revise su "explicación de beneficios" que recibe de su compañía de seguros de salud. Haga un seguimiento con su compañía de seguros o proveedor de atención por cualquier artículo que no reconozca. Si es necesario, comuníquese con el proveedor de atención que figura en la explicación de la declaración de beneficios y solicite copias de los registros médicos desde la fecha del posible acceso (mencionado anteriormente) hasta la fecha actual. Pídale a su compañía de seguros un informe actualizado del año hasta la fecha de todos los servicios pagados por usted. Haga un seguimiento con su compañía de seguros o el proveedor de atención por cualquier artículo que no reconozca.

***SI USTED ES RESIDENTE DEL DISTRITO DE COLUMBIA**:* Puede obtener información sobre cómo evitar el robo de identidad de la FTC o de la Oficina del Fiscal General del Distrito de Columbia. Puede comunicarse con estas oficinas en:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

Office of the Attorney General
441 4th Street, NW
Suite 1100 South
Washington, DC 20001
(202) 727-3400
https://oag.dc.gov/

***SI USTED ES RESIDENTE DE MARYLAND**:* Puede obtener información sobre cómo evitar el robo de identidad de la FTC o de la Oficina del Fiscal General de Maryland. Puede comunicarse con estas oficinas en:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

***SI USTED ES RESIDENTE DE NUEVA YORK**:* Puede obtener información sobre la respuesta a violaciones de seguridad y la prevención y protección contra el robo de identidad de la FTC o de las siguientes agencias del estado de Nueva York:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

New York Attorney General
Consumer Frauds &
Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, New York 12231
(800) 697-1220
www.dos.ny.gov

***SI USTED ES RESIDENTE DE CAROLINA DEL NORTE**:* Puede obtener información sobre cómo prevenir el robo de identidad de la FTC o de la Oficina del Fiscal General de Carolina del Norte. Puede comunicarse con estas oficinas en:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com

***SI USTED ES RESIDENTE DE RHODE ISLAND**:* Puede comunicarse con las fuerzas del orden público estatales o locales para determinar si puede presentar u obtener un informe policial relacionado con este incidente. Además, puede ponerse en contacto con el Fiscal General de Rhode Island en:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
http://www.riag.ri.gov/