CMSP

GOVERNING BOARD

CMSP Letter No.: 15-05
Issue Date: April 24, 2015

TO: ALL COUNTY WELFARE DIRECTORS

CC: ALL COUNTY HEALTH DIRECTORS

SUBJECT: ANTHEM BLUE CROSS DATA BREACH (SPANISH)

The purpose of this All County Letter is to transmit Spanish language versions of the Anthem Blue Cross Data Breach Flyer and Anthem Blue Cross Member Letter included in ACL 15-04 on April 7, 2015. Please refer to ACL 15-04 for information regarding the Anthem Blue Cross data breach of January 29, 2015.

If you have any questions about this letter please contact Jennifer Burkhalter, Office Manager at (916) 649-2631 ext. 21 or jburkhalter@cmspcounties.org.

Thank you,

Kari Brownstein
Administrative Officer

Attachments

County Medical Services Program Governing Board
1451 River Park Drive, Suite 222 • Sacramento, CA 95815
Phone: 916.649.2631 • FAX: 916.649.2606
www.cmspcounties.org

ATENCIÓN

MIEMBROS ANTERIORES DE CMSP Y PATH2HEALTH
USTED PUEDE VERSE AFECTADO POR LA VIOLACIÓN DE DATOS DE ANTHEM

¿Qué pasó?

El 29 de enero de 2015, Anthem Blue Cross (Anthem) se enteró de que se había producido un ciberataque contra su sistema de información electrónica. Los atacantes trataron de obtener información privada sobre miembros de Anthem, tanto actuales como anteriores. A raíz de esto, Anthem tomó medidas para solucionar el problema de seguridad, se dirigió al FBI para iniciar una investigación y contrató a una empresa líder en materia de ciberseguridad (Mandiant) para ayudar con la investigación.

¿Quién se vio afectado?

Miembros actuales o anteriores de CMSP y Path2Health y otros miembros de Anthem.

¿A qué información tuvieron acceso los ciberatacantes?

La información que pudieron haber obtenido incluye los siguientes datos:

- Nombres
- Fechas de nacimiento
- Números de afiliación a la Seguridad Social
- Números de identificación (ID) de servicio de salud
- Direcciones de domicilios
- Direcciones de correo electrónico
- Información laboral, tal como datos de ingresos

¿Qué ayuda está ofreciendo Anthem?

Anthem envió una carta a todos los miembros afectados de CMSP y Path2Health. Si cambió su dirección, quizás no haya recibido la carta. Anthem ha hecho un arreglo con una empresa de protección de identidad, **AllClear ID,** para que proteja la identidad de los miembros afectados de CMSP y Path2Health durante dos años sin costo para sus miembros. Estos servicios de protección de identidad comienzan en la fecha del aviso enviado a los miembros.

Línea directa sin cargo 1-877-263-7995

Anthem ha creado un número directo sin cargo para que los miembros actuales y anteriores de CMSP y Path2Health puedan llamar si tienen preguntas sobre este incidente. Ese número es 1-877-263-7995 o TTY/TDD 1-800-855-2880.

Tenga cuidado con impostores y estafadores

Debe tener cuidado con los correos electrónicos fraudulentos que van dirigidos a miembros actuales y anteriores de Anthem. Estos mensajes fraudulentos se llaman "phishing" y se pretende que parezcan venir de Anthem. Estos correos electrónicos incluyen un enlace que dice "haga clic aquí", para el monitoreo de crédito. Estos correos electrónicos NO han sido enviados por Anthem.

- ***NO*** responda al correo electrónico ni contacte de ninguna manera al remitente.
- ***NO*** ingrese ninguna información en el sitio web que pueda abrirse si ha hecho clic en un enlace del correo electrónico.
- ***NO*** abra ningún archivo adjunto que llegue con el correo electrónico.
- Anthem no está solicitando información sobre su tarjeta de crédito ni su número de afiliación a la Seguridad Social por teléfono.

¿Información adicional o preguntas?
Pídale a su asistente social una copia de la carta de aviso que Anthem ha enviado a miembros de CMSP y Path2Health.

[Date]

Estimado(a) miembro actual o antiguo:

El 29 de enero de 2015, Anthem, Inc. (Anthem) se enteró de un ataque informático a nuestro sistema de TI. Los atacantes informáticos intentaron obtener información privada acerca de miembros actuales y antiguos de Anthem. Pensamos que esto sucedió durante el transcurso de varias semanas comenzando a principios de diciembre de 2014.

Tan pronto nos enteramos sobre el ataque:

- Comenzamos a trabajar para ponerle final a los problemas de seguridad
- Nos pusimos en contacto con el FBI para iniciar una investigación
- Contratamos a Mandiant, una empresa líder de seguridad informática, para que nos ayudara con la investigación

Queremos proporcionarles servicios de protección de identidad a los miembros afectados.

Ataque informático – Un delito que intenta dañar, alterar o tomar datos de una computadora, grupo o red cuando no se ha dado aprobación

Atacantes informáticos – Personas que intentan dañar, alterar o tomar datos de una computadora, un grupo o red de computadoras cuando no se ha dado aprobación

Seguridad informática – Medidas tomadas para proteger datos de que los dañen, alteren o roben de una computadora, sistema o red

¿Quién está afectado?

Los miembros actuales o antiguos de uno de los planes de salud afiliados a Anthem pueden estar afectados. Estos planes incluyen, pero no están limitados a **Amerigroup, UniCare, CareMore y HealthPlus Amerigroup**. Puede visitar anthemfacts.com para ver una lista de planes de Anthem que pueden estar afectados. Anthem es un proveedor de servicios para otros planes de salud grupales y planes de Blue Cross and Blue Shield en todo el país.

Sistema de tecnología informática (TI) – Un grupo o red de computadoras que maneja datos electrónicamente

¿A qué tuvieron acceso los atacantes informáticos?

La información accedida puede haber incluido:

- Nombres
- Fechas de nacimiento
- Números de Seguro Social
- Números de identificación de cuidado de la salud
- Direcciones residenciales
- Direcciones de correo electrónico
- Información laboral como datos de ingresos

Investigación – Investigar lo que sucedió y quién fue parte del problema

No creemos que estas clases de información fueron identificadas o accedidas:

- Información bancaria o de tarjetas de crédito
- Información médica como reclamos, resultados de análisis o códigos de diagnóstico

Servicios de protección de identidad

Hemos hecho arreglos para que AllClear ID proteja su identidad durante dos años sin costo para usted. Estos servicios de protección de identidad inician en la fecha de este aviso. Puede usarlos en cualquier momento durante los próximos dos años.

Servicios de protección de identidad – Una compañía que ayuda a mantener datos personales en privacidad y seguros

- AllClear ID: El equipo en AllClear ID está listo y en espera si usted necesita ayuda para recuperarse del robo de identidad. Le estamos dando este servicio sin costo. No tiene que inscribirse. Si surge un problema, solo tiene que llamar al 1-877-263-7995. Un investigador hará del trabajo de:
  - Recuperar pérdidas financieras
  - Restaurar su crédito
  - Asegurarse de que su identidad sea devuelta a cómo debería ser
- AllClear ID mantiene una calificación de A+ en el Better Business Bureau.
- AllClear PRO: Este servicio ofrece niveles adicionales de protección, incluyendo:
  - Monitoreo de crédito
  - Una póliza de seguro contra robo de identidad de $1 millón
  - Para un niño menor de 18 años, AllClear ID ChildScan encuentra actos de fraude contra niños haciendo búsquedas en archivos de datos de uso de la información de su hijo.
  - Para usar el servicio PRO, deberá proporcionar su información personal a AllClear ID. Para saber más sobre estos servicios o para inscribirse:
- Visite anthemfacts.com
- Haga clic en el enlace de AllClear ID desde ahí

Identidad – Cualquier cosa que haga a alguien distinto de todos los demás

Monitoreo de crédito – Un servicio o una compañía que vigila sus cuentas de tarjeta de crédito contra eventos o cargos extraños

Información personal y privada – Cualquier dato acerca de una persona viva, por ejemplo: nombre, fecha de nacimiento, número de Seguro Social o dirección

Tenga en cuenta: Tal vez deba tomar medidas adicionales para iniciar sus alertas por teléfono.

Aviso enviado por correo

Anthem también les dirá a todos los miembros actuales y antiguos probablemente afectados mediante el Servicio Postal de EE.UU. cómo inscribirse en servicios gratuitos de monitoreo de crédito y protección de identidad. Estos servicios serán brindados gratuitamente. Anthem también ha configurado un sitio web (www.anthemfacts.com) donde usted puede averiguar más. Otros miembros de su hogar también pueden recibir esta carta si están inscritos en un plan de Anthem. Conserve esta carta en un lugar seguro con sus otros documentos importantes.

Línea directa gratuita

Anthem ha configurado un número de línea gratuita para que los miembros actuales y antiguos llamen si tienen preguntas acerca de este incidente. Ese número es 1-877-263-7995 o TTY/TDD 1-800-855-2884. En la próxima página se brinda información de contacto para las tres agencias crediticias nacionales.

Agencia crediticia – Una compañía que guarda datos sobre la forma en que una persona usa su crédito y asigna un puntaje crediticio

Consejos para la prevención de fraudes

Hay medidas que usted puede tomar para resguardarse contra el robo de identidad o fraude.

Fraude – El delito de usar medidas deshonestas para tomar algo de alguna otra persona para ocasionar daño

Exhortamos a los miembros probablemente afectados a que permanezcan alertas por incidentes de fraude y robo de identidad. Esto incluye revisar sus estados de cuenta y verificar informes crediticios gratuitos. Además, usted puede denunciar sospechas de incidentes de robo de identidad a agencias locales de cumplimiento de la ley, a la Comisión Federal de Comercio (Federal Trade Commission [FTC]) o al fiscal general de su estado. Para saber más, puede:

Robo de identidad – Cuando los datos personales han sido tomados por alguien que desea hacer daño

- Ir al sitio web de la FTC en www.consumer.gov/idtheft
- Llamar a la FTC al 1-877-IDTHEFT (1-877-438-4338) o
- Escribir a:
  Federal Trade Commission
  Consumer Response Center
  600 Pennsylvania Avenue NW
  Washington, DC 20580

Informe crediticio – Un informe con información sobre el historial de crédito de una persona

Debe estar pendiente de campañas de estafa por correo electrónico dirigidas a miembros actuales y antiguos de Anthem. Estas estafas se llaman "phishing". Tienen la intención de parecer que vienen de Anthem. Estos correos electrónicos incluyen un enlace de "haga clic aquí" para monitoreo de crédito. **Estos correos electrónicos NO son de Anthem.**

- NO responda al correo electrónico o se comunique con los remitentes de ninguna manera.
- NO ingrese ninguna información en el sitio web que se pueda abrir, si usted hizo clic en el enlace de un correo electrónico.
- NO abra ningún adjunto que llegue con el correo electrónico.

Anthem no está llamando a los miembros acerca del ataque informático. Además, Anthem no está pidiendo información de tarjeta de crédito o números de Seguro Social por teléfono. Para obtener ayuda sobre cómo detectar estafas por correo electrónico, visite el sitio web de la FTC en www.consumer.ftc.gov/articles/0003-phishing.

Información de las agencias crediticias

Equifax	**Experian**	**TransUnion**
PO BOX 740241 ATLANTA, GA 30374-0241 1-800-685-1111 equifax.com	PO BOX 9532 ALLEN, TX 75013 1-888-397-3742 experian.com	PO BOX 6790 CHESTER, PA 19022 1-800-916-8800 transunion.com

Puede obtener más información de la FTC y las agencias crediticias acerca de alertas de fraude y congelamientos de seguridad. Puede añadir una alerta de fraude al expediente de su informe crediticio para ayudar a proteger su información de crédito. Una alerta de fraude puede dificultar más que alguien consiga crédito en su nombre. Esto es porque la misma le dice a los acreedores que sigan ciertos pasos para protegerlo, pero también puede retrasar su capacidad para conseguir crédito.

Alerta de fraude – Una alerta puesta en una cuenta de tarjeta de crédito cuando un evento o cargo no muestra cómo actúa con mayor frecuencia el dueño de la cuenta

Usted puede colocar una alerta de fraude en su expediente llamando a una de las agencias crediticias listadas anteriormente. Cuando esa agencia ayuda a procesar su alerta de fraude, le dirá a las otras dos agencias. Entonces estas también colocarán alertas de fraude en su expediente.

Además, puede visitar los enlaces de las agencias crediticias a continuación para saber si y cómo puede colocar un congelamiento de seguridad en su informe crediticio. Esto puede detener a una agencia crediticia de compartir información de su informe crediticio sin su consentimiento previo por escrito:

Congelamiento de seguridad – Un aviso puesto en el informe crediticio de una persona. Ayuda a protegerlos de ser víctimas de robo de identidad

- Congelamiento de seguridad de Equifax: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
- Congelamiento de seguridad de Experian: www.experian.com/consumer/security_freeze.html
- Congelamiento de seguridad de TransUnion: www.transunion.com/personal-credit/credit-disputes/credit-freezes.page

Para residentes de Maryland y North Carolina — puede obtener información de estas fuentes acerca de ayuda para evitar el robo de identidad:

Comisión Federal de Comercio

- Visite el sitio web de la FTC en www.ftc.gov
- Llame al 1-877-ID-THEFT o
- Escriba a:
  Federal Trade Commission
  600 Pennsylvania Avenue NW
  Washington, DC 20580

Maryland

- Visite el sitio web de la Oficina del Fiscal General de Maryland en www.oag.state.md.us/idtheft/index.htm
- Llame al 1-410-528-8662 o
- Escriba a:
  Consumer Protection Division
  Maryland Office of the Attorney General
  200 St Paul Place
  Baltimore, MD 21202

North Carolina

- Visite el sitio web de la Oficina del Fiscal General de North Carolina en www.ncdoj.gov/Crime.aspx
- Llame al 1-919-716-6400 o
- Escriba a:
  Attorney General's Office
  9001 Mail Service Center
  Raleigh, NC 27699-9001