C/O IDX
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
(833) 726-0930
Or Visit:
https://response.idx.us/srch
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

February 26, 2021

(Data Variable 1 - English)

Dear [Name]:

Santa Rosa Community Health ("SRCH") recently experienced a security incident that may have impacted a limited amount of your protected health information ("PHI"), including your name and Social Security number. We value the privacy and confidentiality of your information and we sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and the resources we are making available to help you.

What happened?

We recently identified suspicious email activity associated with one of our corporate email accounts, and engaged independent computer forensic experts to help us investigate this activity. As part of their investigation, we asked that they review all email accounts in our environment. This review found unauthorized access to one corporate email account that may have impacted your PHI. We engaged a vendor to conduct a comprehensive review of the affected email account and on December 30, 2020, we received a report from the vendor that identified the PHI that may have been stored in the account. We then expended significant time and effort to identify missing contact information and conduct other quality control checks on the data. This process concluded on January 20, 2021. Although we have no evidence that your information has been misused, we wanted to let you know about this incident out of an abundance of caution.

What information was involved?

The review of the email account and its contents determined that your name and Social Security number, in combination with one or more of the following data elements, may have been contained in the account: date of birth, address, health insurance and billing information, and diagnosis and treatment plan. Your bank account and other financial account information was not contained in the email account and remains secure.

What we are doing?

We want to assure you that we are taking steps to prevent this type of incident from happening in the future. We have performed a global password reset for all email accounts, increased our anti-malware and spam filters, implemented multi-factor authentication on all email accounts, and are currently retraining our employees on cybersecurity and on recognizing and responding to suspicious emails.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance

reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What you can do?

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling (833) 726-0930 or going to https://response.idx.us/srch and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. The deadline to enroll is May 26, 2021.

At this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives can answer questions or concerns you may have regarding protection of your personal information. In addition, it is always a good idea to review and monitor your benefits, credit card, and bank statements and immediately report suspicious activity to your financial institution or insurance provider.

For more information:

If you have any questions or concerns, please call (833) 726-0930 Monday through Friday from 6 am – 6 pm Pacific Time. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Greg Spry
IT Director

Naomi Fuchs
Chief Executive Officer

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://response.idx.us/srch and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the CyberScan monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (833) 726-0930 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Watch for Suspicious Activity. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Security Freeze. You may place a free credit freeze for children under age 16. By placing a security freeze, someone who fraudulently acquires your child's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the three national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your child's credit files.

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

6. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: 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.

C/O IDX
P.O. Box 1907
Suwanee, GA 30024

Para inscribirse, llame al:
(833) 726-0930
O visite:
https://response.idx.us/srch
Código de inscripción:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

February 26, 2021

(Data Variable 1 - Spanish)

Estimado/a [Name]:

Santa Rosa Community Health ("SRCH") experimentó recientemente un incidente de seguridad que puede haber afectado una cantidad limitada de su información médica protegida ("PHI"), incluido su nombre y número de seguro social. Valoramos la privacidad y confidencialidad de su información y nos disculpamos sinceramente por cualquier inquietud o inconveniente que esto pueda causarle. Esta carta contiene información sobre las medias que puede tomar para proteger su información y los recursos que ponemos a su disposición para ayudarlo.

¿Qué ocurrió?

Recientemente identificamos actividades sospechosas de correo electrónico asociadas con una de nuestras cuentas de correo electrónico corporativas y contratamos a expertos en informática forense independientes para que nos ayudaran a investigar esta actividad. Como parte de su investigación, les pedimos que revisaran todas las cuentas de correo electrónico de nuestro entorno. Esta revisión detectó acceso no autorizado a una cuenta de correo electrónico corporativa que puede haber afectado su PHI. Contratamos a un proveedor para que realizara una revisión integral de la cuenta de correo electrónico afectada y el 30 de diciembre de 2020 recibimos un informe del proveedor que identificó la PHI que pudo haber sido almacenada en la cuenta. Luego, dedicamos mucho tiempo y esfuerzo a identificar la información de contacto que faltaba y realizar otras verificaciones de control de calidad de los datos. Este proceso concluyó el 20 de enero de 2021. Aunque no tenemos evidencia de que su información haya sido mal utilizada, queremos informarle sobre este incidente por motivos de extrema precaución.

¿Qué información estuvo involucrada?

La revisión de la cuenta de correo electrónico y su contenido determinó que su nombre y número de seguro social, en combinación con uno o más de los siguientes datos, pueden haber estado presentes en la cuenta: fecha de nacimiento, dirección, información de seguro médico y facturación, y diagnóstico y plan de tratamiento. Su información de cuenta bancaria y otra información de cuentas financieras no estaba presente en la cuenta de correo electrónico y permanece a salvo.

¿Qué medidas estamos tomando?

Queremos asegurarle que estamos tomando medidas para evitar que este tipo de incidentes ocurran en el futuro. Hemos realizado un restablecimiento global de contraseñas para todas las cuentas de correo electrónico, hemos aumentado nuestros filtros antimalware y de correo no deseado, hemos implementado la autenticación multifactor en todas las cuentas de correo electrónico y actualmente estamos volviendo a capacitar a nuestros empleados en ciberseguridad y en el reconocimiento y la respuesta a correos electrónicos sospechosos.

Además, ofrecemos servicios de protección contra robo de identidad a través de IDX, el experto en servicios de violación y recuperación de datos. Los servicios de protección de identidad de IDX incluyen: 12 meses de supervisión de crédito y CyberScan, una política de reembolso de $1,000,000 en concepto de seguro y servicios de recuperación de robo de identidad completamente administrados. Con esta protección, IDX lo ayudará a resolver problemas si su identidad está comprometida.

¿Qué puede hacer usted?

Le recomendamos que se ponga en contacto con IDX ante cualquier duda y que se inscriba en los servicios gratuitos de protección de identidad llamando al (833) 726-0930 o visitando el sitio web https://response.idx.us/srch y utilizando el código de inscripción proporcionado anteriormente. Los representantes de IDX están disponibles de lunes a viernes, de 6 a. m. a 6 p. m., Hora del Pacífico. La fecha límite para inscribirse es el 26 de mayo de 2021.

En este momento, no hay evidencia de que su información haya sido utilizada indebidamente. Sin embargo, lo alentamos a aprovechar al máximo esta oferta de servicios. Los representantes de IDX pueden responder preguntas o inquietudes que usted pueda tener con respecto a la protección de su información personal. Además, siempre es una buena idea revisar y controlar sus beneficios, tarjetas de crédito y extractos bancarios e informar inmediatamente cualquier actividad sospechosa a su institución financiera o proveedor de seguros.

Para obtener más información:

Si tiene alguna pregunta o inquietud, llame al (833) 726-0930 de lunes a viernes de 6 a.m. a 6 p.m., Hora del Pacífico. Su confianza es nuestra máxima prioridad y lamentamos profundamente cualquier inconveniente o preocupación que este asunto pueda causarle.

Atentamente.

Greg Spry
Director de TI

Naomi Fuchs
Directora ejecutiva

Pasos recomendados para ayudar a proteger su información

1. **Sitio web e inscripción.** Ingrese en https://response.idx.us/srch y siga las instrucciones para inscribirse con el código de inscripción proporcionado en la parte superior de esta carta.

2. Active el servicio de supervisión de CyberScan proporcionado como parte de su membresía de protección de identidad IDX. El servicio de supervisión incluido en la membresía debe activarse para que entre en vigencia. Nota: Para usar este servicio, deberá tener acceso a una computadora con Internet. Si necesita ayuda, IDX podrá brindarle asistencia.

3. Teléfono. Comuníquese con IDX llamando al (833) 726-0930 para obtener información adicional sobre este evento y para hablar con representantes informados sobre las medidas apropiadas a seguir para proteger su identidad crediticia.

4. Esté atento a actividades sospechosas. Si descubre algún elemento sospechoso y se ha inscrito en el servicio de protección de identidad IDX, notifíquelo de inmediato llamando o iniciando sesión en el sitio web de MyIDCare y presentando una solicitud de ayuda.

Si presenta una solicitud de ayuda o informa actividades sospechosas, un miembro de nuestro equipo de ID Care lo contactará y lo ayudará a determinar la causa de los elementos sospechosos. En el caso improbable de que sea víctima de un robo de identidad como consecuencia de este incidente, se le asignará un Especialista de ID Care que trabajará en su nombre para identificar, detener y revertir el daño rápidamente.

También debe saber que usted tiene derecho a presentar un informe policial si alguna vez experimenta un robo de identidad o fraude. Tenga en cuenta que, para presentar un informe de delito o incidente ante las autoridades policiales por robo de identidad, es probable que deba proporcionar algún tipo de prueba de que ha sido víctima de dicho evento. A menudo se requiere un informe policial para disputar elementos fraudulentos. Puede informar cualquier presunto incidente de robo de identidad a la policía local o al Fiscal General.

5. Congelamiento de seguridad. Puede colocar un congelamiento de crédito gratuito para jóvenes menores de 16 años de edad. Al aplicar un congelamiento de seguridad, cualquier persona que adquiera de manera fraudulenta la información de identificación personal de su hijo no podrá usar dicha información para abrir nuevas cuentas ni para pedir dinero prestado a su nombre. Deberá ponerse en contacto con las tres agencias nacionales de informes de crédito mencionadas a continuación para aplicar el congelamiento. Tenga en cuenta que, cuando aplique el congelamiento, no podrá pedir dinero prestado, obtener crédito instantáneo ni obtener una nueva tarjeta de crédito hasta que levante temporalmente o elimine en forma permanente el congelamiento. Puede congelar o descongelar los archivos de crédito de su hijo sin costo alguno.

Agencias 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 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

6. Usted puede obtener información adicional sobre los pasos que puede seguir para evitar el robo de identidad de las siguientes agencias. La Comisión Federal de Comercio también anima a que aquellos que descubren que su información ha sido utilizada indebidamente presenten una queja ante dicha institución.

Residentes de California: Visite la Oficina de Protección de la Privacidad de California (www.oag.ca.gov/privacy) para obtener información adicional sobre la protección contra el robo de identidad.

Residentes de Kentucky: Oficina del Fiscal General de Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Teléfono: 1-502-696-5300.

Residentes de Maryland: Oficina del Fiscal General de Maryland**,** División de Protección al Consumidor 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Teléfono: 1-888-743-0023.

Residentes de Nuevo México: Conforme a la Ley de Informe Imparcial de Crédito (*Fair Credit Reporting Act*), usted tiene ciertos derechos, tales como el derecho a que se le notifique si la información en su archivo de crédito ha sido utilizada en su contra, el derecho a saber qué hay en dicho archivo, el derecho a solicitar su puntaje de crédito, y el derecho a disputar información incompleta o inexacta. Además, conforme a la Ley de Informe Imparcial de Crédito: las agencias de informes crediticios deben corregir o eliminar la información inexacta, incompleta o no verificable; dichas agencias no pueden reportar información negativa desactualizada; el acceso a su archivo es limitado; usted debe dar su consentimiento para que se proporcionen informes de crédito a los empleadores; usted puede limitar las ofertas de crédito y seguro "preseleccionadas" que recibe según la información de su informe crediticio; y puede reclamar daños y perjuicios de un infractor. También podría tener otros derechos conforme a la Ley de Informe Imparcial de Crédito que no están resumidos en este documento. Las víctimas de robo de identidad y el personal militar en servicio activo tienen derechos adicionales específicos de conformidad con la ley mencionada anteriormente. Puede revisar sus derechos de conformidad con la Ley de Informe Imparcial de Crédito, visitando www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, o bien; escribiendo un correo a Centro de Respuesta al Consumidor, Sala 130-A, Comisión Federal de Comercio, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Residentes de Nueva York: puede comunicarse con el Fiscal General en: Oficina del Fiscal General, El Capitolio, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

Residentes de Carolina del Norte: Oficina del Fiscal General de Carolina del Norte**,** 9001 Centro de servicio de correo Raleigh, NC 27699-9001, www.ncdoj.gov, Teléfono: 1-919-716-6400.

Residentes de Oregon: Departamento de Justicia de Oregon, 1162 Court Street NE, Salem, O 97301-4096, www.doj.state.or.us/, Teléfono: 877-877-9392

Residentes de Rhode Island: Oficina del Fiscal General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Teléfono: 401-274-4400

Todos los residentes de los Estados Unidos: Centro de Información de Robo de Identidad, Comisión Federal de Comercio, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.