Rady Children's Hospital San Diego

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

RE: Notice of Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

As part of the community of patients who have been in our care, we need to let you know about a data security incident involving patient health information. We are disclosing this event to you in that you have the right to this information, and we want to be transparent about what occurred.

What Happened: On January 3, 2020, we learned of a data security incident that involved radiology-related patient information. Upon learning of the incident, we secured the affected information and launched an immediate investigation. We learned that, between the dates of June 20, 2019 and January 3, 2020, some information for a limited number of patients was accessed without authorization via an Internet port. On February 5, 2020, our investigation determined that your information may have been involved.

What Information Was Involved: The information that was involved is listed below but did NOT include Social Security numbers, credit card numbers, radiology images, radiology reports, or diagnoses. Instead, the patient information included patient name, gender, and type and date of imaging studies. In some instances, the patient information also included one or more of the following types of information: date of birth, medical record number, description of the imaging study, and the referring physician's name.

What We Are Doing: As soon as we learned of this incident, we took the measures referenced above. We also engaged a digital forensics firm to assist with our investigation. In partnership with that firm, we are continuing to take steps to further protect the security of patient information and to ensure a similar incident does not occur in the future. In addition, we are notifying the appropriate state and federal regulatory agencies. With this letter, we wanted to notify you of the incident, offer you complimentary identity protection services for 12 months, and provide you with steps you can take to protect your personal information.

What You Can Do: You can enroll in the identity protection services that we are offering for 12 months at no charge through Experian. The services we are offering, known as Experian IdentityWorks, include Internet surveillance to monitor the trading of your personal information on the Internet, identity restoration services, and identity theft insurance. To enroll in the complimentary services, please visit https://www.experianidworks.com/identity, provide your activation code **<<Member ID>>**, and other information when prompted. If you have questions about the product, need assistance with identity restoration, or would like an alternative to online enrollment, please contact Experian's customer care team at 877.288.8057 by **<<b2b_text_1(EnrollmentDeadline)>>**. Be prepared to provide engagement number **<<b2b_text_2(EngagementNumber)>>** as proof of eligibility. You can also follow the other recommendations included with this letter to protect your personal information.

For More Information: If you have any questions about this letter, please call 1-844-902-2025, 8:00 a.m. to 5:00 p.m. Pacific Time. You may also consult the resources included on the following page, which provides information about how to protect your personal information.

We regret that this incident occurred and extend our sincerest apologies. The security of patient information remains a top priority at Rady Children's.

Sincerely,

Christina Galbo, MBA, CHC
Chief Compliance and Privacy Officer

Rady Children's Hospital San Diego

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

RE: Notificación de incidente de seguridad en la protección de datos

Estimado/a <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Como parte de la comunidad de pacientes que han estado bajo nuestro cuidado, deseamos informarle sobre un incidente de seguridad en la protección de sus datosde salud. Le informamos de este suceso porque tiene derecho a recibir esta información y porque queremos ser transparentes sobre lo ocurrido.

Qué ha sucedido: El 3 de enero de 2020 supimos que hubo un incidente de seguridad en la protección de datos radiologicós de pacientes. En cuanto tuvimos conocimiento del incidente aseguramos la información afectada e iniciamos una investigación inmediata. Averiguamos que, entre las fechas del 20 de junio de 2019 y el 3 de enero de 2020, se accedió sin autorización, a través de un puerto de internet, a cierta información de un número limitado de pacientes. Determinamos en nuestra investigación del 5 de febrero de 2020 que su información podría haber sido involucrada.

Qué información ha sido afectada: La información implicada se menciona abajo, pero NO incluyó los números de seguro social, de tarjetas de crédito, imágenes de radiología, informes de radiología ni diagnósticos. En cambio, incluyó el nombre del paciente, su género y el tipo y fecha de los estudios radiológicos realizados. En algunos casos, también incluyó uno o más de los siguientes datos: fecha de nacimiento, número de expediente médico, descripción del estudio radiológico o nombre del médico de referencia.

Qué estamos haciendo: En cuanto tuvimos conocimiento de este incidente tomamos las medidas arriba mencionadas. También contratamos a una empresa de investigación forense digital para ayudarnos con nuestra investigación. En colaboración con esa empresa, continuamos tomando pasos para proteger aún más la seguridad de la información de los datos, con el fin de asegurar que no vuelva a ocurrir en el futuro un incidente similar. Además, estamos notificando a las autoridades competentes, estatales y federales. Con esta carta, queremos informarle del incidente, ofrecerle servicios gratuitos de protección de identidad por 12 meses, y darle información de las medidas que puede tomar para proteger su información personal.

Qué puede hacer usted: Se puede inscribir en los servicios de protección de identidad que ofrecemos por 12 meses, sin ningún costo, a través de Experian. Los servicios que ofrecemos, conocidos como Experian IdentityWorks, incluyen vigilancia de internet para supervisar el intercambio de su información personal en internet, servicios de restauración de identidad y seguro contra robo de identidad. Para inscribirse en estos servicios gratuitos, visite https://www.experianidworks.com/identity, facilite su código de activación **<<Member ID>>**, y otra información que le pidan. Si tiene preguntas sobre el producto, necesita ayuda con la restauración de identidad o desea una alternativa a la inscripción en línea, llame al equipo de atención al cliente de Experian al 877.288.8057 antes del **<<b2b_text_1(EnrollmentDeadline)>>**. Esté preparado para facilitar el número de participación **<<b2b_text_2(EngagementNumber)>>** como prueba de eligibilidad. También puede seguir las recomendaciones incluídas en esta carta para proteger su información personal.

Si desea más información: Si tiene cualquier pregunta sobre esta carta, por favor llame al 1-844-902-2025, de 8:00 a.m. a 5:00 p. m. hora del Pacífico. También puede consultar los recursos incluídos en la siguiente página, que le brindan información sobre cómo proteger su información personal.

Lamentamos este incidente y le expresamos nuestras más sinceras disculpas. La seguridad de datos de nuestros pacientes continúa siendo una prioridad para Rady Children's.

Atentamente,

Christina Galbo, MBA, CHC
Chief Compliance and Privacy Officer

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 740241	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374	Atlanta, GA 30348
1-800-916-8800	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their attorneys general using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft.

Medidas que puede tomar para proteger aún más su información

Revise sus estados de cuenta y notifique a los agentes del orden público sobre cualquier actividad sospechosa: como medida de precaución, le recomendamos que se mantenga alerta revisando atentamente sus estados de cuenta e informes de crédito. Si detecta alguna actividad sospechosa en una cuenta, debe notificar de inmediato a la institución financiera o empresa en la que tiene la cuenta. También debe informar rápidamente de cualquier actividad fraudulenta o cualquier caso sospechoso de robo de identidad a las autoridades policiales competentes, al fiscal general de su estado y/o a la Comisión Federal de Comercio (Federal Trade Commission, FTC).

Copia del informe de crédito: puede obtener una copia gratuita de su informe de crédito de cada una de las tres principales agencias de informes de crédito una vez cada 12 meses si visita la página http://www.annualcreditreport.com/, llama a la línea gratuita 877-322-8228, o completa un Formulario de Solicitud de Informes de Crédito Anuales y lo envía por correo al Servicio de Solicitud de Informes de Crédito Anuales (Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348). Puede encontrar el formulario en https://www.annualcreditreport.com/cra/requestformfinal.pdf. También puede ponerse en contacto con una de las siguientes tres agencias nacionales de informes de crédito:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 740241	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374	Atlanta, GA 30348
1-800-916-8800	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Alerta de fraudes: puede considerar la posibilidad de colocar una alerta de fraude en su informe crediticio. La alerta de fraude inicial es gratuita y permanecerá en su archivo de crédito por lo menos durante un año. La alerta informa a los acreedores sobre una posible actividad fraudulenta en su informe y solicita que el acreedor se comunique con usted antes de establecer cualquier cuenta en su nombre. Para colocar una alerta de fraude en su informe crediticio, comuníquese con cualquiera de las tres agencias de informes crediticios mencionadas anteriormente. Puede obtener información adicional en http://www.annualcreditreport.com.

Bloqueo de seguridad: de acuerdo con la ley de los Estados Unidos, usted tiene el derecho de poner un bloqueo de seguridad en su archivo de crédito por hasta un año sin costo alguno. Esto evitará que se abran nuevos créditos a su nombre sin el uso de un número PIN que se le otorga cuando inicia el bloqueo. El bloqueo de seguridad está destinado a evitar que los posibles acreedores accedan a su informe crediticio sin su consentimiento. Como resultado, el uso de un bloqueo de seguridad puede interferir o retrasar su capacidad de obtener crédito. Usted debe colocar por separado un bloqueo de seguridad en su archivo de crédito con cada agencia de informes de crédito. Para poder colocar un bloqueo de seguridad, se le puede requerir que proporcione a la agencia de reportes del consumidor información que lo identifique, incluyendo su nombre completo, número de Seguro Social, fecha de nacimiento, dirección actual y anterior, una copia de su tarjeta de identificación emitida por el estado, y una factura reciente de servicios públicos, un estado de cuenta bancario o un estado de cuenta del seguro.

Recursos gratuitos adicionales: puede obtener información de las agencias de informes de los consumidores, de la FTC o del respectivo fiscal general de su estado sobre alertas de fraude, bloqueos de seguridad y medidas que puede tomar para prevenir el robo de identidad. Usted puede denunciar una sospecha de robo de identidad a la policía local, incluyendo a la Comisión Federal de Comercio o al fiscal general de su estado. Los residentes de Maryland, Carolina del Norte y Rhode Island pueden obtener más información de sus fiscales generales utilizando la información de contacto que aparece a continuación.

Federal Trade Commission (Comisión Federal de Comercio)	**Maryland Attorney General (Fiscal General de Maryland)**	**North Carolina Attorney General (Fiscal General de Carolina del Norte)**	**Rhode Island Fiscal General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, y	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

También tiene ciertos derechos según la Ley de Información Crediticia Justa (Fair Credit Reporting Act, FCRA): estos incluyen el derecho a conocer lo que hay en su expediente; a disputar información incompleta o inexacta; a que las agencias de informes de los consumidores corrijan o eliminen la información inexacta, incompleta o no verificable. Para obtener más información sobre la FCRA, y sus derechos en virtud de la FCRA, por favor visite http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf

Información personal de un menor: puede solicitar que cada una de las tres agencias nacionales de informes de crédito realice una búsqueda manual del número de Seguro Social de un menor para determinar si existe un informe de crédito asociado. Se pueden requerir copias de la información de identificación del menor y del padre/tutor, incluyendo el certificado de nacimiento o de adopción, la tarjeta de Seguro Social y la tarjeta de identificación emitida por el gobierno. Si existe un informe crediticio, debe solicitar una copia del mismo y denunciar inmediatamente de cualquier cuenta fraudulenta a la agencia de informes crediticios. También puede denunciar cualquier uso indebido de la información de un menor a la FTC en https://www.identitytheft.gov/. Para obtener más información sobre el Robo de Identidad de Menores y las instrucciones para solicitar una búsqueda manual de número de Seguro Social, visite el sitio web de la FTC: https://www.consumer.ftc.gov/articles/0040-child-identity-theft.