[HOSPITAL LOGO] [FOUNDATION LOGO]

3020 Children's Way, San Diego, CA 92123

[DATE]

[NAME]
[ADDRESS1]
[ADDRESS2]
[CITY] [STATE] [ZIP]

Re: Notice of Data Security Incident

Dear [NAME],

As part of the Rady Children's community, we wanted to let you know about an incident that one of our third-party service providers, Blackbaud, Inc. ("Blackbaud"), experienced, and which involved your personal information. Although this incident involved data hosted by a third-party vendor, Rady Children's Hospital – San Diego and the Rady Children's Hospital Foundation – San Diego are providing you this information because we appreciate the sensitive nature of this issue, and we want to be transparent about what we understand occurred.

What Happened: Blackbaud recently informed us that it experienced a data security incident that may have involved information pertaining to members of our community who provided information to Rady Children's Hospital – San Diego or the Rady Children's Hospital Foundation – San Diego. Upon learning of the incident, we immediately launched an investigation to determine what happened and whether any personal information was impacted. According to Blackbaud, between February 7, 2020 and June 4, 2020, an unauthorized party had access to backup files related to the Blackbaud fundraising and donor management software we use. Upon learning this information, we retained outside cybersecurity experts, including a vendor to review the backup data at issue. On October 7, 2020, we determined that some of your personal information was contained in the backup files. Blackbaud has informed us that it has no reason to believe that any information in the files has been or will be misused, or will otherwise be made available publicly. We nonetheless wanted to make you aware of this incident and offer you complimentary identity monitoring services to help alleviate any concern you may have.

What Information Was Involved: Although Blackbaud has informed us that it has no indication that any of your information was actually viewed by an unauthorized person, the incident may have involved the following information, which may be different for different individuals. The information could include: <<*insert variable text*>>.

What We Are Doing: As soon as we learned of the incident, we launched an investigation. We also worked with Blackbaud to obtain additional information regarding the incident and to confirm that it was taking steps to ensure that the information at issue was not being misused, and that it was taking steps to further protect our information going forward. Blackbaud has represented that they are monitoring the dark web for any exchange of personal information related to this incident, but have found no indication that the information is available on the dark web. Blackbaud also stated that they have reported the incident to the Federal Bureau of Investigation (FBI). We will offer the FBI and law enforcement whatever assistance is needed. In addition, we are notifying you of the incident and providing you with steps you can take to protect your personal information, including by enrolling in the complimentary services that we are offering.

What You Can Do: You can follow the recommendations included with this letter for other steps you can take to protect your personal information. You can also enroll in the complimentary identity monitoring services that we are offering 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 <<CODE>>, 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 January 18, 2021. Be prepared to provide engagement number B005864 as proof of eligibility.

[HOSPITAL LOGO] [FOUNDATION LOGO]

3020 Children's Way, San Diego, CA 92123

For More Information: If you have any questions about this letter, please call [CALL CENTER NUMBER], x:00 a.m. to x:00 p.m. Pacific Time. You may also consult the resources included on the following pages, which provide information about how to protect your personal information.

We regret any concern caused by this incident involving Blackbaud. The security of information for members of our community remains a top priority for Rady Children's Hospital – San Diego and the Rady Children's Hospital Foundation – San Diego.

Sincerely,

Christina Galbo, MBA, CHC
Chief Compliance and Privacy Officer

[HOSPITAL LOGO] [FOUNDATION LOGO]

3020 Children's Way, San Diego, CA 92123

29 de octubre de 2020

[NAME]
[ADDRESS1]
[ADDRESS2]
[CITY] [STATE] [ZIP]

Re: Notificación acerca de un incidente de seguridad de datos

Estimado [NAME]:

Como parte de la comunidad de Rady Children, queremos informarle acerca de un incidente que ha experimentado uno de nuestros proveedores externos, Blackbaud, Inc. ("Blackbaud"), y que ha involucrado su información personal. Aunque este incidente implicó datos albergados por un tercer proveedor, el Hospital de Rady Children – San Diego y la Fundación del Hospital de Rady Children – San Diego le facilitan esta información porque apreciamos la delicada naturaleza de este problema y porque queremos ser transparentes sobre lo que entendemos que ocurrió.

Qué sucedió: Blackbaud recientemente nos informó que experimentó un incidente de seguridad de datos que pudo haber involucrado información de miembros de nuestra comunidad que proporcionaron información al Hospital de Rady Children – San Diego o a la Fundación del Hospital de Rady Children – San Diego. Al conocer el incidente, inmediatamente pusimos en marcha una investigación para determinar lo sucedido y saber si impactó a alguna información personal. Según Blackbaud, entre el 7 de febrero de 2020 y el 4 de junio de 2020, una parte no autorizada tuvo acceso a archivos de seguridad relacionados con recaudación de fondos de Blackbaud y software de gestión de donantes. Al conocer esta información, contratamos a expertos externos de seguridad cibernética, incluyendo a un proveedor para revisar los datos de seguridad implicados. El 7 de octubre de 2020 determinamos que alguna de su información personal estaba contenida en los archivos de seguridad. Blackbaud nos ha informado de que no tiene motivo para creer que se haya dado un mal uso a ninguna información de los archivos, que se vaya a hacer un mal uso de la misma o que se vaya a hacer pública. A pesar de todo esto, queríamos informarle de este incidente y ofrecerle servicios de supervisión de identidad gratuitos para ayudar a mitigar cualquier preocupación que pueda tener.

Qué información estuvo implicada: Aunque Blackbaud nos ha informado de que no tiene indicación de que ninguna de su información fuera vista por ninguna persona no autorizada, el incidente pudo haber involucrado la siguiente información, que podría ser diferente para distintos individuos. La información podría incluir: *<<insert variable text>>*.

Qué estamos haciendo: En cuanto tuvimos conocimiento de este incidente, pusimos en marcha una investigación. También trabajamos con Blackbaud para obtener información adicional del incidente y para confirmar que estaba tomando los pasos necesarios para asegurar que la información del caso no estaba siendo mal utilizada, y que estaba tomando los pasos necesarios para proteger más nuestra información a partir de ese momento. Blackbaud ha comunicado que están monitorizando la página web oscura por cualquier intercambio de información personal relacionada con este incidente, pero que no ha encontrado ninguna indicación de que la información esté disponible en la página oscura. Blackbaud también ha indicado que ha denunciado el incidente a la Oficina Federal de Investigación (Federal Bureau of Investigation, o FBI, por sus siglas en inglés). Ofreceremos al FBI y a las fuerzas policiales cualquier ayuda que necesiten. Además, le estamos notificando el incidente e indicándole los pasos que puede tomar para proteger su información personal, incluyendo el inscribirse en los servicios complementarios que ofrecemos.

Qué puede hacer: Usted puede seguir las recomendaciones incluídas en esta carta sobre otros pasos que puede tomar para proteger su información personal. También se puede inscribir en los servicios complementarios de vigilancia de identidad que estamos ofreciendo a través de Experian. Los servicios que estamos ofreciendo, conocidos como Experian IdentityWorks, incluyen vigilancia a través de internet para monitorizar el intercambio de

la información personal de su hijo en internet, servicios de reestablecimiento de identidad y seguro de robo de identidad. Para inscribirse en los servicios complementarios, visite https://www.experianidworks.com/identity, proporcione su código de activación <<CODE>> y otra información solicitada. Si tiene cualquier pregunta del producto, necesita ayuda con el reestablecimiento de identidad o le gustaría que le dieran una alternativa a la matriculación en línea, contacte por favor con el equipo de atención al cliente de Experian en el número 877-288-8057 antes del 18 de enero de 2021.Esté preparado para facilitar el número de participación B005864 como prueba de eligibilidad.

Para obtener más información: Si tiene cualquier pregunta sobre esta carta, llame al [CALL CENTER NUMBER], de x:00 a. m. a x:00 p. m. hora del Pacífico. También puede consultar los recursos incluídos en las siguientes páginas, que proporcionan información sobre cómo proteger su información personal.

Lamentamos cualquier preocupación causada por este incidente que ha involucrado a Blackbaud. La seguridad de la información de los miembros de nuestra comunidad sigue siendo nuestra máxima prioridad en el Hospital de Rady Children – San Diego y Fundación del Hospital Rady Children – San Diego.

Atentamente,

Christina Galbo, MBA, CHC
Chief Compliance and Privacy Officer

[HOSPITAL LOGO] [FOUNDATION LOGO]

3020 Children's Way, San Diego, CA 92123

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 90 days. 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.

[HOSPITAL LOGO] [FOUNDATION LOGO]

3020 Children's Way, San Diego, CA 92123

Medidas que puede tomar para proteger aún más su información

Revise sus p 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 90 días. 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	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Fiscal General**
(Comisión Federal de Comercio)	(Fiscal General de Maryland)	(Fiscal General de Carolina del Norte)	150 South Main Street
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	Providence, RI 02903
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	http://www.riag.ri.gov
consumer.ftc.gov, y	oag.state.md.us	ncdoj.gov	401-274-4400
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	
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.