20192

HEALTH CENTER PARTNERS
of Southern California

C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE
NAME
ADDRESS1
ADDRESS2
CSZ
BREAK
SEQ
CODE 2D
Ver 2
COUNTRY

April 12, 2021

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a recent data security incident experienced by Netgain Technology, LLC ("Netgain"), the IT service provider for Health Center Partners of Southern California ("HCP"). HCP supports community health centers in a variety of ways, including collaborative grant-funded programs and services for <<HEALTHCENTER>>. Please read this letter carefully as it contains information regarding the incident, the type of information potentially involved, and the steps that you can take to help protect your personal information.

What Happened: Netgain recently informed HCP that it had experienced a data security incident that involved systems containing HCP data. Upon its discovery of the incident, Netgain brought all of its systems offline and engaged outside cybersecurity experts to conduct an investigation and to assist in its mitigation, restoration, and remediation efforts. Once HCP learned of the incident, we engaged our own independent cybersecurity experts to determine what happened, whether any HCP data was compromised as a result of the incident, and the impact of this incident on HCP, our health center members and partners, and their patients.

According to Netgain, in late September 2020, an unauthorized third party gained access to Netgain's digital environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain's cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

Once we learned that HCP data may have been involved in the incident, we worked with our cybersecurity experts to review the impacted files and identify the individuals whose information was contained in such files so that we may notify such individuals. Our investigation revealed that the impacted files contained your personal information. **Again, we are not aware of any misuse of your personal information as a result of this incident.** Nevertheless, we are notifying you about this incident out of an abundance of caution and providing you with steps you can take to help protect your information.

What Information Was Involved: The information involved varies depending on the individual but may include the following: <<VARPARAGRAPH>>. **Your Social Security number was not impacted by this incident.**

What We Are Doing: As soon as we learned of the incident, we took the steps described above. In addition, we worked with Netgain to confirm that it was taking steps to ensure that the information at issue was not being misused and that it has implemented additional measures to enhance the security of its digital environment in an effort to minimize the likelihood of a similar event from occurring in the future. Furthermore, we have reported the incident to law enforcement

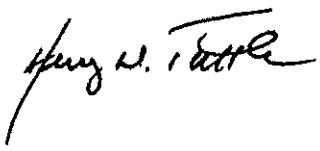
agencies, including the Federal Bureau of Investigation, and we are committed to assisting their investigation into the matter.

What You Can Do: As we have stated, we are not aware of any misuse of your information as a result of this incident. However, we encourage you to follow the recommendations on the next page to help protect your information.

For More Information: If you have any questions regarding the incident, please call 1-833-416-0926 between 6:00 a.m. and 6:00 p.m. Pacific Time.

The security of your information is a top priority for HCP, and we are committed to safeguarding your data and privacy.

Sincerely,



Henry Tuttle, President & Chief Executive Officer
Health Center Partners of Southern California

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 also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.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 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.

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
www.consumer.ftc.gov, and	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	1-401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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; as well as other rights. 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.

HEALTH CENTER PARTNERS
of Southern California

C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE

NAME
ADDRESS1
ADDRESS2
CSZ
BREAK
1
CODE 2D
5
COUNTRY

To Enroll, Please Call:
1-833-416-0926
Or Visit:
https://response.idx.us/hcp-netgain-incident
Enrollment Code: <<XXXXXXXX>>

April 12, 2021

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a recent data security incident experienced by Netgain Technology, LLC ("Netgain"), the IT service provider for Health Center Partners of Southern California ("HCP"). HCP supports community health centers in a variety of ways, including collaborative grant-funded programs and services for <<HEALTHCENTER>>. Please read this letter carefully as it contains information regarding the incident, the type of information potentially involved, and the steps that you can take to help protect your personal information.

What Happened: Netgain recently informed HCP that it had experienced a data security incident that involved systems containing HCP data. Upon its discovery of the incident, Netgain brought all of its systems offline and engaged outside cybersecurity experts to conduct an investigation and to assist in its mitigation, restoration, and remediation efforts. Once HCP learned of the incident, we engaged our own independent cybersecurity experts to determine what happened, whether any HCP data was compromised as a result of the incident, and the impact of this incident on HCP, our health center members and partners, and their patients.

According to Netgain, in late September 2020, an unauthorized third party gained access to Netgain's digital environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain's cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

Once we learned that HCP data may have been involved in the incident, we worked with our cybersecurity experts to review the impacted files and identify the individuals whose information was contained in such files so that we may notify such individuals. Our investigation revealed that the impacted files contained your personal information. **Again, we are not aware of any misuse of your personal information as a result of this incident.** Nevertheless, we are notifying you about this incident out of an abundance of caution and providing you with steps you can take to help protect your information.

What Information Was Involved: The information involved varies depending on the individual but may include the following: <<VARPARAGRAPH>>.

What We Are Doing: As soon as we learned of the incident, we took the steps described above. In addition, we worked with Netgain to confirm that it was taking steps to ensure that the information at issue was not being misused and that it has implemented additional measures to enhance the security of its digital environment in an effort to minimize the likelihood of a similar event from occurring in the future. Furthermore, we have reported the incident to law enforcement agencies, including the Federal Bureau of Investigation, and we are committed to assisting their investigation into the matter.

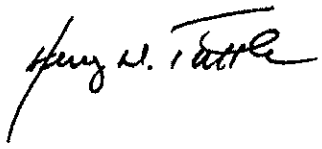
We are providing you with steps that you can take to help protect your personal information, and as an added precaution, we are offering you complimentary identity protection services through IDX, a leader in risk mitigation and response. These services include xx months of credit monitoring, dark web monitoring, a $1,000,000 identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

What You Can Do: As we have stated, we are not aware of any misuse of your information as a result of this incident. However, we encourage you to follow the recommendations on the next page to help protect your information. We also encourage you to enroll in the complimentary services offered by going to https://response.idx.us/hcp-netgain-incident or calling 1-833-416-0926 and using the enrollment code provided above. Please note that the deadline to enroll is July 12, 2021.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call 1-833-416-0926 between 6:00 a.m. and 6:00 p.m. Pacific Time.

The security of your information is a top priority for HCP, and we are committed to safeguarding your data and privacy.

Sincerely,



Henry Tuttle, President & Chief Executive Officer
Health Center Partners of Southern California

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 also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.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 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.

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
www.consumer.ftc.gov, and	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	1-401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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; as well as other rights. 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.

HEALTH CENTER PARTNERS
of Southern California

C/O IDX
PO Box 4129
Everett WA 98204

NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

Para inscribirse, llame al:
1-833-416-0926
O visitar:
https://response.idx.us/hcp-netgain-incident
Código de inscripción: <<XXXXXXXX>>

12 de abril de 2021

Ref.: Aviso de violación de datos

Estimando(a) <<First Name>> <<Last Name>>:

Le escribo para informarle sobre un incidente de seguridad de datos que le sucedió recientemente a Netgain Technology, LLC ("Netgain"), el proveedor de servicios de tecnología de Health Center Partners of Southern California ("HCP"). HCP provee apoyo a los centros de salud comunitarios en varias maneras, incluyendo programas y servicios colaborativos financiados por subvenciones para <<HEALTHCENTER>>. Por favor lea esta carta detenidamente, ya que contiene información sobre el incidente, el tipo de información potencialmente involucrada y los pasos que puede tomar para proteger su información personal.

Qué sucedió: Netgain informó recientemente a HCP que le había sucedido un incidente de seguridad de datos que involucraba sistemas que contenían datos de HCP. Tras su descubrimiento del incidente, Netgain desconectó todos sus sistemas y contrató a expertos en ciberseguridad para que investiguen y asisten con sus esfuerzos de mitigación, restauración y remediación. En cuanto HCP se enteró del incidente, contratamos a nuestros propios expertos en ciberseguridad para determinar qué sucedió, si los datos del HCP fueron comprometidos a resultado del incidente y el impacto de este incidente en HCP, los miembros y socios de nuestro centro de salud y sus pacientes.

Netgain nos informó que, a fines de septiembre de 2020, otra persona sin autorización obtuvo acceso al entorno digital de Netgain, y entre el 22 de octubre de 2020 y el 3 de diciembre de 2020, esa personal sin autorización obtuvo ciertos archivos que contenían datos de HCP. Netgain nos informa que le pagó una cantidad no revelada al atacante a cambio de garantías de que el atacante eliminará todas las copias de estos datos y que no publicará, venderá ni divulgará los datos. Además, los expertos en ciberseguridad de Netgain buscaron en la red obscura los archivos afectados, pero dichas búsquedas no han resultado en ninguna indicación de que los datos involucrados en este incidente hayan sido o serán publicados, vendidos, puestos a la venta o divulgados de otra manera. Por lo tanto, no hay razón para creer que cualquier información involucrada en el incidente haya sido o será mal utilizada.

En cuanto supimos que los datos del HCP pudieron haber estado involucrados en el incidente, trabajamos con nuestros expertos en ciberseguridad para revisar los archivos afectados e identificar a las personas cuya información estaba contenida en dichos archivos para poder notificar a dichas personas. Nuestra investigación reveló que los archivos afectados contenían su información personal. **Nuevamente, no tenemos conocimiento de ningún mal uso de su información personal debido a este incidente**. Sin embargo, queremos notificarle sobre este incidente por precaución y para infórmale de los pasos que puede tomar para ayudar a proteger su información.

Qué información estuvo involucrada: La información potencialmente involucrada varía según la persona, pero puede incluir lo siguiente: <<VARPARAGRAPH>>.

Qué estamos haciendo: En cuanto nos enteramos del incidente, tomamos los pasos descritos anteriormente. Además, trabajamos con Netgain para confirmar que estaba tomando medidas para garantizar que la información en cuestión no fue

mal utilizada y que había implementado medidas adicionales para mejorar la seguridad de su entorno digital en un esfuerzo para reducir la probabilidad de que ocurra un problema similar en el futuro. Además, hemos informado a las agencias de policía y seguridad, incluyendo la Oficina Federal de Investigaciones, y estamos comprometidos a ayudarles en la investigación del asunto.

Le proveemos información de los pasos que puede tomar para ayudar a proteger su información personal y, como precaución adicional, le ofrecemos servicios de protección de identidad complementarios a través de IDX, un líder en mitigación de riesgos y la respuesta. Estos servicios incluyen xx meses de monitoreo de crédito, monitoreo de la red oscura, una póliza de reembolso de pérdida de identidad causada por fraude de $1,000,000 y servicios de recuperación de robo de identidad que son completamente administrados por especialistas.

Qué puede hacer: Como le hemos dicho, no tenemos conocimiento de ningún uso indebido de su información como resultado de este incidente. Sin embargo, le recomendamos que siga las recomendaciones de la página siguiente para ayudar a proteger su información. También lo alentamos a que se inscriba en los servicios complementarios que se ofrecen en la página de red: https://response.idx.us/hcp-netgain-incident o llamando al 1-833-416-0926 y utilizando el código de inscripción proporcionado arriba. Tenga en cuenta que el plazo para inscribirse es 12 de julio de 2021.

Para obtener más información: Si usted tiene alguna pregunta sobre el incidente o si desea ayuda para inscribirse en los servicios ofrecidos, llame al 1-833-416-0926 entre las 6:00 a.m. y las 6:00 p.m. hora del Pacífico.

La seguridad de su información es una prioridad alta para HCP, y estamos comprometidos a proteger sus datos y privacidad.

Atentamente,

Henry Tuttle
President & Chief Executive Officer
Health Center Partners of Southern California

Pasos que puede tomar para proteger aún más su información

Revise sus estados de cuenta y notifique a las autoridades de policía de actividades sospechosas: Como 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 con la que se mantiene la cuenta. También debe informar de inmediato cualquier actividad fraudulenta o cualquier sospecha de robo de identidad a las autoridades de policía, al fiscal general de su estado y/o a la Comisión Federal de Comercio/ Federal Trade Commission (FTC).

Copia del su reporte de crédito: Usted puede obtener una copia gratuita de su reporte de cada una de las tres agencias principales de informes crédito una vez cada 12 meses. Lo puede pedir en la página de red: http://www.annualcreditreport.com/, llamando al número gratuito 877-322-8228 o llenando un formulario de solicitud de reporte de crédito anual/ Annual Credit Report Request Form y enviándolo por correo a: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. También puede comunicarse con una de las siguientes tres agencias nacionales de informes de crédito:

TransUnion	**Experian**	**Equifax**
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.com

Alerta de fraude: Es posible que desee considerar colocar una alerta de fraude en su informe de crédito. Una alerta de fraude inicial es gratuita y permanecerá en su archivo de crédito por un año. La alerta informa a los acreedores de una posible actividad fraudulenta dentro de su informe y solicita que el acreedor se comunique con usted antes de establecer cuentas a su nombre. Para colocar una alerta de fraude en su informe de crédito, comuníquese con cualquiera de las tres agencias de informes de crédito identificadas anteriormente. Información adicional está disponible en la página de red: http://www.annualcreditreport.com.

Congelamiento de seguridad: Según la ley de los EE. UU., usted tiene derecho a congelar su archivo de crédito hasta un año sin ningún costo. Esto evitará que se abra un nuevo crédito a su nombre sin el uso de un número de PIN que se le dará cuando inicie la congelación. Un congelamiento de seguridad está diseñado para evitar que los acreedores potenciales accedan a su informe de crédito sin su consentimiento. El uso de un congelamiento de seguridad puede interferir o retrasar su capacidad de obtener crédito. Debe colocar un congelamiento de seguridad separado en su archivo de crédito con cada agencia de informes de crédito. Para colocar un congelamiento de seguridad, es posible que se le solicite que proporcione a la agencia de informes del consumidor información que lo identifique, incluyendo su nombre completo, número de seguro social, fecha de nacimiento, dirección actual y anteriores, una copia de su tarjeta de identificación del estado y una factura de servicios públicos, un estado bancario o de seguro recientes.

Recursos gratuitos adicionales: Usted puede obtener información de las agencias de informes del consumidor, la FTC o de su Fiscal General estatal sobre alertas de fraude, congelamientos de seguridad y pasos que puede tomar para prevenir el robo de identidad. Puede reporte la sospecha de robo de identidad a la policía local, incluso a la FTC o al Fiscal General de su estado.

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
www.consumer.ftc.gov, and	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	1-401-274-4400
1-877-438-4338			

También tiene ciertos derechos bajo la Ley de Informe Justo de Crédito/ Fair Credit Reporting Act (FCRA): Estos derechos incluyen saber qué hay en su archivo; para disputar información incompleta o inexacta; hacer que las agencias de informes del consumidor corrijan o eliminen información inexacta, incompleta o no verificable; así como otros derechos. Para obtener más información sobre la FCRA y sus derechos, visite la página de red: http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

HEALTH CENTER PARTNERS
of Southern California

C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE

NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

SEQ
CODE 2D
Ver 6

BREAK

April 12, 2021

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a recent data security incident experienced by Netgain Technology, LLC ("Netgain"), the IT service provider for Health Center Partners of Southern California ("HCP"). HCP supports community health centers in a variety of ways, including collaborative grant-funded programs and services for <<HEALTHCENTER>>. Please read this letter carefully as it contains information regarding the incident, the type of information potentially involved, and the steps that you can take to help protect your personal information.

What Happened: Netgain recently informed HCP that it had experienced a data security incident that involved systems containing HCP data. Upon its discovery of the incident, Netgain brought all of its systems offline and engaged outside cybersecurity experts to conduct an investigation and to assist in its mitigation, restoration, and remediation efforts. Once HCP learned of the incident, we engaged our own independent cybersecurity experts to determine what happened, whether any HCP data was compromised as a result of the incident, and the impact of this incident on HCP, our health center members and partners, and their patients.

According to Netgain, in late September 2020, an unauthorized third party gained access to Netgain's digital environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain's cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

Once we learned that HCP data may have been involved in the incident, we worked with our cybersecurity experts to review the impacted files and identify the individuals whose information was contained in such files so that we may notify such individuals. Our investigation revealed that the impacted files contained your personal information. **Again, we are not aware of any misuse of your personal information as a result of this incident.** Nevertheless, we are notifying you about this incident out of an abundance of caution and providing you with steps you can take to help protect your information.

What Information Was Involved: The information involved varies depending on the individual but may include the following: <<VARPARAGRAPH>>. **Your Social Security number was not impacted by this incident.**

What We Are Doing: As soon as we learned of the incident, we took the steps described above. In addition, we worked with Netgain to confirm that it was taking steps to ensure that the information at issue was not being misused and that it has implemented additional measures to enhance the security of its digital environment in an effort to minimize the likelihood of

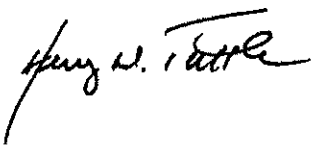
a similar event from occurring in the future. Furthermore, we have reported the incident to law enforcement agencies, including the Federal Bureau of Investigation, and we are committed to assisting their investigation into the matter.

What You Can Do: As we have stated, we are not aware of any misuse of your information as a result of this incident. However, we encourage you to follow the recommendations on the next page to help protect your information.

For More Information: If you have any questions regarding the incident, please call 1-833-416-0926 between 6:00 a.m. and 6:00 p.m. Pacific Time.

The security of your information is a top priority for HCP, and we are committed to safeguarding your data and privacy.

Sincerely,



Henry Tuttle, President & Chief Executive Officer
Health Center Partners of Southern California

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 also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.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 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.

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

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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; as well as other rights. 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.

HEALTH CENTER PARTNERS
of Southern California

C/O IDX
PO Box 4129
Everett WA 98204

NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

12 de abril de 2021

Ref.: Aviso de violación de datos

Estimando(a) <<First Name>> <<Last Name>>:

Le escribo para informarle sobre un incidente de seguridad de datos que le sucedió recientemente a Netgain Technology, LLC ("Netgain"), el proveedor de servicios de tecnología de Health Center Partners of Southern California ("HCP"). HCP provee apoyo a los centros de salud comunitarios en varias maneras, incluyendo programas y servicios colaborativos financiados por subvenciones para <<HEALTHCENTER>>. Por favor lea esta carta detenidamente, ya que contiene información sobre el incidente, el tipo de información potencialmente involucrada y los pasos que puede tomar para proteger su información personal.

Qué sucedió: Netgain informó recientemente a HCP que le había sucedido un incidente de seguridad de datos que involucraba sistemas que contenían datos de HCP. Tras su descubrimiento del incidente, Netgain desconectó todos sus sistemas y contrató a expertos en ciberseguridad para que investiguen y asisten con sus esfuerzos de mitigación, restauración y remediación. En cuanto HCP se enteró del incidente, contratamos a nuestros propios expertos en ciberseguridad para determinar qué sucedió, si los datos del HCP fueron comprometidos a resultado del incidente y el impacto de este incidente en HCP, los miembros y socios de nuestro centro de salud y sus pacientes.

Netgain nos informó que, a fines de septiembre de 2020, otra persona sin autorización obtuvo acceso al entorno digital de Netgain, y entre el 22 de octubre de 2020 y el 3 de diciembre de 2020, esa personal sin autorización obtuvo ciertos archivos que contenían datos de HCP. Netgain nos informa que le pagó una cantidad no revelada al atacante a cambio de garantías de que el atacante eliminará todas las copias de estos datos y que no publicará, venderá ni divulgará los datos. Además, los expertos en ciberseguridad de Netgain buscaron en la red obscura los archivos afectados, pero dichas búsquedas no han resultado en ninguna indicación de que los datos involucrados en este incidente hayan sido o serán publicados, vendidos, puestos a la venta o divulgados de otra manera. Por lo tanto, no hay razón para creer que cualquier información involucrada en el incidente haya sido o será mal utilizada.

En cuanto supimos que los datos del HCP pudieron haber estado involucrados en el incidente, trabajamos con nuestros expertos en ciberseguridad para revisar los archivos afectados e identificar a las personas cuya información estaba contenida en dichos archivos para poder notificar a dichas personas. Nuestra investigación reveló que los archivos afectados contenían su información personal. **Nuevamente, no tenemos conocimiento de ningún mal uso de su información personal debido a este incidente**. Sin embargo, queremos notificarle sobre este incidente por precaución y para infórmale de los pasos que puede tomar para ayudar a proteger su información.

Qué información estuvo involucrada: La información potencialmente involucrada varía según la persona, pero puede incluir lo siguiente: <<VARPARAGRAPH_S1>><<VARPARAGRAPH_S2>>. **Su número de Seguro Social no fue afectado por este incidente.**

Qué estamos haciendo: En cuanto nos enteramos del incidente, tomamos los pasos descritos anteriormente. Además, trabajamos con Netgain para confirmar que estaba tomando medidas para garantizar que la información en cuestión no fue mal utilizada y que había implementado medidas adicionales para mejorar la seguridad de su entorno digital en un esfuerzo para reducir la probabilidad de que ocurra un problema similar en el futuro. Además, hemos informado a las agencias de

policía y seguridad, incluyendo la Oficina Federal de Investigaciones, y estamos comprometidos a ayudarles en la investigación del asunto.

Qué puede hacer: Como le hemos dicho, no tenemos conocimiento de ningún uso indebido de su información como resultado de este incidente. Sin embargo, le recomendamos que siga las recomendaciones de la página siguiente para ayudar a proteger su información.

Para obtener más información: Si usted tiene alguna pregunta sobre el incidente, llame al 1-833-416-0926 entre las 6:00 a.m. y las 6:00 p.m. hora del Pacífico.

La seguridad de su información es una prioridad alta para HCP, y estamos comprometidos a proteger sus datos y privacidad.

Atentamente,

Henry Tuttle, President & Chief Executive Officer
Health Center Partners of Southern California

Pasos que puede tomar para proteger aún más su información

Revise sus estados de cuenta y notifique a las autoridades de policía de actividades sospechosas: Como 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 con la que se mantiene la cuenta. También debe informar de inmediato cualquier actividad fraudulenta o cualquier sospecha de robo de identidad a las autoridades de policía, al fiscal general de su estado y/o a la Comisión Federal de Comercio/ Federal Trade Commission (FTC).

Copia del su reporte de crédito: Usted puede obtener una copia gratuita de su reporte de cada una de las tres agencias principales de informes crédito una vez cada 12 meses. Lo puede pedir en la página de red: http://www.annualcreditreport.com/, llamando al número gratuito 877-322-8228 o llenando un formulario de solicitud de reporte de crédito anual/ Annual Credit Report Request Form y enviándolo por correo a: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. También puede comunicarse con una de las siguientes tres agencias nacionales de informes de crédito:

TransUnion	**Experian**	**Equifax**
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.com

Alerta de fraude: Es posible que desee considerar colocar una alerta de fraude en su informe de crédito. Una alerta de fraude inicial es gratuita y permanecerá en su archivo de crédito por un año. La alerta informa a los acreedores de una posible actividad fraudulenta dentro de su informe y solicita que el acreedor se comunique con usted antes de establecer cuentas a su nombre. Para colocar una alerta de fraude en su informe de crédito, comuníquese con cualquiera de las tres agencias de informes de crédito identificadas anteriormente. Información adicional está disponible en la página de red: http://www.annualcreditreport.com.

Congelamiento de seguridad: Según la ley de los EE. UU., usted tiene derecho a congelar su archivo de crédito hasta un año sin ningún costo. Esto evitará que se abra un nuevo crédito a su nombre sin el uso de un número de PIN que se le dará cuando inicie la congelación. Un congelamiento de seguridad está diseñado para evitar que los acreedores potenciales accedan a su informe de crédito sin su consentimiento. El uso de un congelamiento de seguridad puede interferir o retrasar su capacidad de obtener crédito. Debe colocar un congelamiento de seguridad separado en su archivo de crédito con cada agencia de informes de crédito. Para colocar un congelamiento de seguridad, es posible que se le solicite que proporcione a la agencia de informes del consumidor información que lo identifique, incluyendo su nombre completo, número de seguro social, fecha de nacimiento, dirección actual y anteriores, una copia de su tarjeta de identificación del estado y una factura de servicios públicos, un estado bancario o de seguro recientes.

Recursos gratuitos adicionales: Usted puede obtener información de las agencias de informes del consumidor, la FTC o de su Fiscal General estatal sobre alertas de fraude, congelamientos de seguridad y pasos que puede tomar para prevenir el robo de identidad. Puede reporte la sospecha de robo de identidad a la policía local, incluso a la FTC o al Fiscal General de su estado.

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
www.consumer.ftc.gov, and	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	1-401-274-4400
1-877-438-4338			

También tiene ciertos derechos bajo la Ley de Informe Justo de Crédito/ Fair Credit Reporting Act (FCRA): Estos derechos incluyen saber qué hay en su archivo; para disputar información incompleta o inexacta; hacer que las agencias de informes del consumidor corrijan o eliminen información inexacta, incompleta o no verificable; así como otros derechos. Para obtener más información sobre la FCRA y sus derechos, visite la página de red: http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

HEALTH CENTER PARTNERS
of Southern California

C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE

To the Parent or Guardian of
NAME
ADDRESS1
ADDRESS2
SEQ
CODE 2D CSZ BREAK
Ver 8 COUNTRY

April 12, 2021

Re: Notice of Data Breach

Dear Parent or Guardian of <<First Name>> <<Last Name>>:

I am writing to inform you of a recent data security incident experienced by Netgain Technology, LLC ("Netgain"), the IT service provider for Health Center Partners of Southern California ("HCP"). HCP supports community health centers in a variety of ways, including collaborative grant-funded programs and services for <<HEALTHCENTER>>. Please read this letter carefully as it contains information regarding the incident, the type of information potentially involved, and the steps that you can take to help protect your child's personal information.

What Happened: Netgain recently informed HCP that it had experienced a data security incident that involved systems containing HCP data. Upon its discovery of the incident, Netgain brought all of its systems offline and engaged outside cybersecurity experts to conduct an investigation and to assist in its mitigation, restoration, and remediation efforts. Once HCP learned of the incident, we engaged our own independent cybersecurity experts to determine what happened, whether any HCP data was compromised as a result of the incident, and the impact of this incident on HCP, our health center members and partners, and their patients.

According to Netgain, in late September 2020, an unauthorized third party gained access to Netgain's digital environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain's cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

Once we learned that HCP data may have been involved in the incident, we worked with our cybersecurity experts to review the impacted files and identify the individuals whose information was contained in such files so that we may notify such individuals. Our investigation revealed that the impacted files contained your child's personal information. **Again, we are not aware of any misuse of your child's personal information as a result of this incident.** Nevertheless, we are notifying you about this incident out of an abundance of caution and providing you with steps you can take to help protect your child's information.

What Information Was Involved: The information involved varies depending on the individual but may include the following: <<VARPARAGRAPH>>. **Your child's Social Security number was not involved in this incident.**

What We Are Doing: As soon as we learned of the incident, we took the steps described above. In addition, we worked with Netgain to confirm that it was taking steps to ensure that the information at issue was not being misused and that it has implemented additional measures to enhance the security of its digital environment in an effort to minimize the

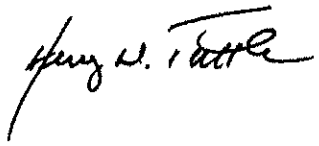
likelihood of a similar event from occurring in the future. Furthermore, we have reported the incident to law enforcement agencies, including the Federal Bureau of Investigation, and we are committed to assisting their investigation into the matter.

What You Can Do: As we have stated, we are not aware of any misuse of your child's information as a result of this incident. However, we encourage you to follow the recommendations on the next page to help protect your child's information.

For More Information: If you have any questions regarding the incident, please call 1-833-416-0926 between 6:00 a.m. and 6:00 p.m. Pacific Time.

The security of your child's information is a top priority for HCP, and we are committed to safeguarding your child's data and privacy.

Sincerely,



Henry Tuttle, President & Chief Executive Officer
Health Center Partners of Southern California

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 also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.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 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.

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
www.consumer.ftc.gov, and	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	1-401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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; as well as other rights. 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.

HEALTH CENTER PARTNERS
of Southern California

C/O IDX
PO Box 4129
Everett WA 98204

NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

12 de abril de 2021

Ref.: Aviso de violación de datos

Estimados padre o tutore de <<First Name>> <<Last Name>>:

Le escribo para informarle sobre un incidente de seguridad de datos que le sucedió recientemente a Netgain Technology, LLC ("Netgain"), el proveedor de servicios de tecnología de Health Center Partners of Southern California ("HCP"). HCP provee apoyo a los centros de salud comunitarios en varias maneras, incluyendo programas y servicios colaborativos financiados por subvenciones para <<HEALTHCENTER>>. Por favor lea esta carta detenidamente, ya que contiene información sobre el incidente, el tipo de información potencialmente involucrada y los pasos que puede tomar para proteger la información personal de su hijo.

Qué sucedió: Netgain informó recientemente a HCP que le había sucedido un incidente de seguridad de datos que involucraba sistemas que contenían datos de HCP. Tras su descubrimiento del incidente, Netgain desconectó todos sus sistemas y contrató a expertos en ciberseguridad para que investiguen y asisten con sus esfuerzos de mitigación, restauración y remediación. En cuanto HCP se enteró del incidente, contratamos a nuestros propios expertos en ciberseguridad para determinar qué sucedió, si los datos del HCP fueron comprometidos a resultado del incidente y el impacto de este incidente en HCP, los miembros y socios de nuestro centro de salud y sus pacientes.

Netgain nos informó que, a fines de septiembre de 2020, otra persona sin autorización obtuvo acceso al entorno digital de Netgain, y entre el 22 de octubre de 2020 y el 3 de diciembre de 2020, esa personal sin autorización obtuvo ciertos archivos que contenían datos de HCP. Netgain nos informa que le pagó una cantidad no revelada al atacante a cambio de garantías de que el atacante eliminará todas las copias de estos datos y que no publicará, venderá ni divulgará los datos. Además, los expertos en ciberseguridad de Netgain buscaron en la red obscura los archivos afectados, pero dichas búsquedas no han resultado en ninguna indicación de que los datos involucrados en este incidente hayan sido o serán publicados, vendidos, puestos a la venta o divulgados de otra manera. Por lo tanto, no hay razón para creer que cualquier información involucrada en el incidente haya sido o será mal utilizada.

En cuanto supimos que los datos del HCP pudieron haber estado involucrados en el incidente, trabajamos con nuestros expertos en ciberseguridad para revisar los archivos afectados e identificar a las personas cuya información estaba contenida en dichos archivos para poder notificar a dichas personas. Nuestra investigación reveló que los archivos afectados contenían la información personal de su hijo. **Nuevamente, no tenemos conocimiento de ningún mal uso de la información personal de su hijo debido a este incidente**. Sin embargo, queremos notificarle sobre este incidente por precaución y para infórmale de los pasos que puede tomar para ayudar a proteger.

Qué información estuvo involucrada: La información potencialmente involucrada varía según la persona, pero puede incluir lo siguiente: <<VARPARAGRAPH_S1>><<VARPARAGRAPH_S2>>. **La número de Seguro Social de su hijo no fue afectado por este incidente.**

Qué estamos haciendo: En cuanto nos enteramos del incidente, tomamos los pasos descritos anteriormente. Además, trabajamos con Netgain para confirmar que estaba tomando medidas para garantizar que la información en cuestión no fue mal utilizada y que había implementado medidas adicionales para mejorar la seguridad de su entorno digital en un esfuerzo para reducir la probabilidad de que ocurra un problema similar en el futuro. Además, hemos informado a las agencias de

policía y seguridad, incluyendo la Oficina Federal de Investigaciones, y estamos comprometidos a ayudarles en la investigación del asunto.

Qué puede hacer: Como le hemos dicho, no tenemos conocimiento de ningún uso indebido de la información personal de su hijo como resultado de este incidente. Sin embargo, le recomendamos que siga las recomendaciones de la página siguiente para ayudar a proteger la información personal de su hijo.

Para obtener más información: Si usted tiene alguna pregunta sobre el incidente, llame al 1-833-416-0926 entre las 6:00 a.m. y las 6:00 p.m. hora del Pacífico.

La seguridad de la información personal de su hijo es una prioridad alta para HCP, y estamos comprometidos a proteger los datos de su hijo y privacidad.

Atentamente,

Henry Tuttle, President & Chief Executive Officer
Health Center Partners of Southern California

Pasos que puede tomar para proteger aún más su información

Revise sus estados de cuenta y notifique a las autoridades de policía de actividades sospechosas: Como 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 con la que se mantiene la cuenta. También debe informar de inmediato cualquier actividad fraudulenta o cualquier sospecha de robo de identidad a las autoridades de policía, al fiscal general de su estado y/o a la Comisión Federal de Comercio/ Federal Trade Commission (FTC).

Copia del su reporte de crédito: Usted puede obtener una copia gratuita de su reporte de cada una de las tres agencias principales de informes crédito una vez cada 12 meses. Lo puede pedir en la página de red: http://www.annualcreditreport.com/, llamando al número gratuito 877-322-8228 o llenando un formulario de solicitud de reporte de crédito anual/ Annual Credit Report Request Form y enviándolo por correo a: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. También puede comunicarse con una de las siguientes tres agencias nacionales de informes de crédito:

TransUnion	**Experian**	**Equifax**
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.com

Alerta de fraude: Es posible que desee considerar colocar una alerta de fraude en su informe de crédito. Una alerta de fraude inicial es gratuita y permanecerá en su archivo de crédito por un año. La alerta informa a los acreedores de una posible actividad fraudulenta dentro de su informe y solicita que el acreedor se comunique con usted antes de establecer cuentas a su nombre. Para colocar una alerta de fraude en su informe de crédito, comuníquese con cualquiera de las tres agencias de informes de crédito identificadas anteriormente. Información adicional está disponible en la página de red: http://www.annualcreditreport.com.

Congelamiento de seguridad: Según la ley de los EE. UU., usted tiene derecho a congelar su archivo de crédito hasta un año sin ningún costo. Esto evitará que se abra un nuevo crédito a su nombre sin el uso de un número de PIN que se le dará cuando inicie la congelación. Un congelamiento de seguridad está diseñado para evitar que los acreedores potenciales accedan a su informe de crédito sin su consentimiento. El uso de un congelamiento de seguridad puede interferir o retrasar su capacidad de obtener crédito. Debe colocar un congelamiento de seguridad separado en su archivo de crédito con cada agencia de informes de crédito. Para colocar un congelamiento de seguridad, es posible que se le solicite que proporcione a la agencia de informes del consumidor información que lo identifique, incluyendo su nombre completo, número de seguro social, fecha de nacimiento, dirección actual y anteriores, una copia de su tarjeta de identificación del estado y una factura de servicios públicos, un estado bancario o de seguro recientes.

Recursos gratuitos adicionales: Usted puede obtener información de las agencias de informes del consumidor, la FTC o de su Fiscal General estatal sobre alertas de fraude, congelamientos de seguridad y pasos que puede tomar para prevenir el robo de identidad. Puede reporte la sospecha de robo de identidad a la policía local, incluso a la FTC o al Fiscal General de su estado.

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
www.consumer.ftc.gov, and	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	1-401-274-4400
1-877-438-4338			

También tiene ciertos derechos bajo la Ley de Informe Justo de Crédito/ Fair Credit Reporting Act (FCRA): Estos derechos incluyen saber qué hay en su archivo; para disputar información incompleta o inexacta; hacer que las agencias de informes del consumidor corrijan o eliminen información inexacta, incompleta o no verificable; así como otros derechos. Para obtener más información sobre la FCRA y sus derechos, visite la página de red: 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.

PCL XL error

Subsystem: GE_VECTOR

Error: GEEmptyClipPath Warning: IllegalMediaSize

3710 Ruffin Rd, San Diego, CA 92123

NOTICE OF DATA SECURITY INCIDENT

Date: April 9, 2021
Media Contact: Allen Sattler (Allen.Satter@lewisbrisbois.com | 714.668.5572)

Health Center Partners of Southern California ("HCP") recently learned of a data security incident experienced by HCP's IT service provider, Netgain Technology, LLC ("Netgain"), involving personal information relating to patients of HCP members and partner organizations.

Once HCP learned of the incident, it engaged its own independent cybersecurity experts to determine what happened, whether any HCP data was compromised as a result of the incident, and the impact of this incident on HCP, its health center partners, and their patients.

According to Netgain, in late September 2020, an unauthorized third party gained access to Netgain's digital environment, and between October 22, 2020 and December 3, 2020, the unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain's cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, **there is no reason to believe that any information involved in the incident has been or will be misused.**

Once HCP learned that its data may have been involved in the incident, HCP took steps to identify the individuals whose information was contained in such files and their current mailing addresses in order to provide written notification. On March 16, 2021, HCP informed affected health center partners—including Borrego Health, Clinicas de Salud del Pueblo, Community Health Systems, Inc., Imperial Beach Community Clinic, Indian Health Council, La Maestra Community Health Centers, Mountain Health (now a part of San Ysidro Health), Neighborhood Healthcare, San Diego American Indian Health Center, San Diego Family Care, San Ysidro Health, St. Vincent de Paul Village Health Center, TrueCare, and Vista Community Clinic—that information relating to some of their patients were contained in the impacted files. The information contained in the impacted files vary depending on the individual but may include the following: name, address, date of birth, diagnosis/treatment information, provider name, medical record number, Medicare/Medicaid number, health insurance number, and treatment cost information. For a small subset of patients, their Social Security number and prescription information may have been contained in the impacted files. Credit/debit card information was involved for fewer than 20 patients.

HCP has confirmed that Netgain has taken steps to ensure that the information at issue was not being misused and that it has implemented additional measures to enhance the security of its digital environment in an effort to minimize the likelihood of a similar event from occurring in the future. Furthermore, HCP reported the incident to law enforcement agencies, including the Federal Bureau of Investigation, and HCP is committed to assisting their investigation into the matter.

Individuals who receive a notification letter pertaining to this matter should review the steps outlined in the letter to protect their personal information. These steps may include reviewing account statements, obtaining copies of credit reports, placing fraud alerts on credit reports, and placing security freezes on credit files. HCP has established a toll-free call center to answer questions about the incident and to address any concerns. Call center representatives are available Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time and can be reached at 1-833-416-0926.

The privacy and security of our patients' personal and protected health information is a top priority for HCP and its health center partners, and we deeply regret any inconvenience or concern this incident may cause.

<<HEALTH CENTER>> Notifies Patients of Data Security Incident

<<CITY>>, CA: April 8, 2021 – <<HEALTH CENTER>> recently learned of a data security incident experienced by Netgain Technology, LLC ("Netgain"), the IT service provider for Health Center Partners of Southern California ("HCP"). HCP supports community health centers in a variety of ways, including collaborative grant-funded programs and services for <<HEALTH CENTER>>. HCP has sent notification of this incident to potentially impacted individuals and has provided resources to assist them.

What Happened: Netgain recently informed HCP that it had experienced a data security incident that involved systems containing HCP data. Upon its discovery of the incident, Netgain brought all of its systems offline and engaged outside cybersecurity experts to conduct an investigation and to assist in its mitigation, restoration, and remediation efforts. Once HCP learned of the incident, it engaged its own independent cybersecurity experts to determine what happened, whether any HCP data was compromised as a result of the incident, and the impact of this incident on HCP, its health center partners, including <<HEALTH CENTER>>, and their patients.

According to Netgain, in late September 2020, an unauthorized third party gained access to Netgain's digital environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain's cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, **there is no reason to believe that any information involved in the incident has been or will be misused.**

Once HCP learned that its data may have been involved in the incident, HCP took steps to identify the individuals whose information was contained in such files and their current mailing addresses in order to provide notification. On March 16, 2021, HCP informed <<HEALTH CENTER>> that information relating to some of our patients was contained in the impacted files. Again, **we not aware of any misuse of your personal information as a result of this incident.** Nevertheless, out of an abundance of caution, HCP and <<HEALTH CENTER>> worked together to send notification letters to potentially impacted patients on April 8, 2021.

What Information Was Involved: The information contained in the impacted files vary depending on the individual but may include the following: <<VARIABLE TEXT1>>. For a small subset of patients, their <<VARIABLE TEXT2>> may have been contained in the impacted files.

What We Are Doing: HCP worked with Netgain to confirm that it was taking steps to ensure that the information at issue was not being misused and that it has implemented additional measures to enhance the security of its digital environment in an effort to minimize the likelihood of a similar event from occurring in the future. Furthermore, HCP reported the incident to law enforcement agencies, including the Federal Bureau of Investigation, and HCP and <<HEALTH CENTER>> are committed to assisting their investigation into the matter.

What You Can Do: The notification letters that were sent to potentially affected individuals include resources and steps that they can take to help protect their personal and protected health information. HCP and <<HEALTH CENTER>> have established a toll free call center to answer questions about the incident and to address any concerns. Call center representatives are available Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time and can be reached at 1-833-416-0926.

The privacy and security of our patients' personal and protected health information is a top priority for <<HEALTH CENTER>>, and we deeply regret any inconvenience or concern this incident may cause.

While HCP and <<HEALTH CENTER>> ***have no evidence of the misuse of any potentially affected individuals' information, it is providing the following information to help those who want to know more about steps they can take to protect themselves and their personal information:***

What steps can I take to protect my personal information?

- Please notify your financial institution immediately if you detect any suspicious activity on any of your accounts, including unauthorized transactions or new accounts opened in your name that you do not recognize. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.
- You can request a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To do so, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is listed at the bottom of this page.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.
- Additional information on what you can do to better protect yourself is included in your notification letter.

How do I obtain a copy of my 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 also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.com

How do I put a fraud alert on my account?
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 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.

How do I put a security freeze on my credit reports?
You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or online by following the instructions found at the websites listed below. You will need to provide the following information when requesting a security freeze (note that if you are making a request for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; and (4) address. You may also be asked to provide other personal information such as your email address, a copy of a government-issued identification card, and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. There is no charge to place, lift, or remove a freeze. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
PO Box 105788	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-909-8872
www.equifax.com	www.experian.com	www.transunion.com

What should I do if my family member's information was involved in the incident and is deceased?
You may choose to notify the three major credit bureaus, Equifax, Experian and TransUnion, and request they flag the deceased credit file. This will prevent the credit file information from being used to open credit. To make this request, mail a copy of your family member's death certificate to each company at the addresses below.

Equifax	**Experian**	**TransUnion**
Equifax Information Services	Experian Information Services	Trans Union Information Services
P.O. Box 105169,	P.O. Box 9701	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022

What should I do if my minor child's information involved in the incident?
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 a 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. Contact information for the three national credit reporting agencies may be found above.