La Clínica
La Clínica de La Raza, Inc.
Mailing Address: Post Office Box 22210 Oakland, CA 94623 • Tel 510-535-4000 • Fax 510-535-4189 • www.laclinica.org

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: Notice of Data Security Incident

Dear <<Name 1>>:

This letter is to inform you of a recent data security incident that may have involved your personal information maintained by La Clinica de la Raza ("La Clinica"). This letter describes the incident, outlines measures that we have taken in response to the incident and provides information regarding additional steps you can take to help protect your information.

What Happened?

On January 28, 2021, La Clinica became aware that malware had been deployed on certain La Clinica systems which store information, including personal information, for the organization. Upon learning of the incident, La Clinica immediately took steps to stop access to these systems, including permanently disconnecting the affected systems from other La Clinica systems and its overall network. La Clinica also began an immediate investigation of the incident with the support of a third-party forensics company. On February 26, 2021, La Clinica's investigation determined that the malware was deployed by an unauthorized individual or entity who gained unauthorized access to La Clinica's systems. Upon learning of the unauthorized access, La Clinica immediately took additional mitigation steps and security measures, including deploying additional measures to monitor the organization's systems and technology infrastructure.

What Information Was Involved?

La Clinica's ongoing investigation has determined that unauthorized access to the affected systems occurred, and ended, on January 12, 2021. Based on the investigation to date, we reasonably believe that relatively few documents were likely viewed by the unauthorized party. However, our investigation could not definitively conclude that the unauthorized party did not access, use or disclose certain information and documents stored in the affected La Clinica systems, which may have included some of the following information: your full name, date of birth, phone number, home address, health insurance information, and certain health information such as dates of service, diagnosis, test results, and treatment information related to care received at La Clinica. Social security numbers and financial account information were not stored in the affected systems and therefore were not involved in this incident. Further, based on our investigation and security practices, we have no reason to believe that there has been any improper access to La Clinica's electronic medical record or billing systems.

What Are We Doing?

La Clinica has taken, and will continue to take, steps to prevent this type of incident from happening again, including enhancing our data security, implementing additional technology safeguards including enhanced intrusion detection and prevention, securing login credentials, enhanced workforce training, and other cybersecurity risk prevention measures. We have also reviewed our security policies and procedures to ensure that they sufficiently protect against further incidents of this type. In addition, we notified federal law enforcement authorities about the incident and will continue to cooperate with their investigation.

What You Can Do.

Please review the enclosed *Information About Identity Theft Protection* section included with this letter. This section describes steps you can take to help protect your identity, including recommendations by the Federal Trade Commission regarding identify theft protection and details on how to place a fraud alert or a security freeze on your credit file if you wish to do so.

For More Information.

We sincerely regret any inconvenience or concern caused by this incident. We take our responsibility to protect the personal information of our patients very seriously. If you have questions or concerns about this incident, please call 855-654-0864, Monday through Friday, between 6:00a.m. and 6:00p.m. Pacific Time.

Sincerely

Fernando Cortez
Chief Information Officer & Information Security Officer

Information About Identity Theft Protection

Monitor Your Accounts
We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®	**Experian**	**TransUnion®**
P.O. Box 740241	P.O. Box 9701	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013-9701	Chester, PA 19016-1000
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze
You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.equifax.com/personal/ credit-report-services	www.experian.com/ freeze/center.html	www.transunion.com/ credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts
You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com/personal/ credit-report-services	www.experian.com/ fraud/center.html	www.transunion.com/ fraud-victim-resource/place-fraud-alert

Monitor Your Personal Health Information
If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at https://oag.ca.gov/privacy/ to find more information about protecting your privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

La Clínica
La Clínica de La Raza, Inc.
Mailing Address: Post Office Box 22210 Oakland, CA 94623 • Tel 510-535-4000 • Fax 510-535-4189 • www.laclinica.org

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: Notificacion Del Incidente De Seguridad Proteccion De Datos

Dear <<Name 1>>:

Esta carta es para informarle de un incidente reciente de seguridad que puede haber involucrado su información personal mantenida por La Clinica de La Raza (La Clinica). Esta carta describe el incidente y las medidas que hemos tomado en repuesta a esta situación y proporciona información sobre los pasos adicionales que puede tomar para ayudar a proteger su información.

¿Que Sucedió?

El 28 de enero del 2021, La Clinica se dio cuenta que se había implementado un programa maligno (malware) en ciertos sistemas de La Clinica que guardan información, incluyendo información personal para la organización. Al enterarse del incidente, La Clinica inmediatamente tomo medidas para parar el acceso a estos sistemas, incluyendo la desconexión permanente de los sistemas afectados de otros sistemas de La Clínica y su red general. La Clínica también inició una investigación inmediata del incidente con el apoyo de una empresa forense. El 26 de febrero de 2021, la investigación de La Clínica determinó que el programa maligno (malware) fue implementado por una persona o entidad no autorizada que obtuvo acceso no autorizado a los sistemas de La Clínica. Al enterarse del acceso no autorizado, La Clínica inmediatamente tomó medidas de mitigación y medidas de seguridad adicionales, incluyendo la implementación de medidas adicionales para monitorear los sistemas y la infraestructura tecnológica de la organización.

¿Que información estuvo involucrada?

La investigación en curso de La Clinica, ha determinado que el acceso no autorizado a los sistemas afectados ocurrió y termino el 12 de enero de 2021. Basado en nuestra investigación hasta la fecha, creemos razonablemente que la persona o entidad que no estaba autorizada probablemente nomas vieron relativamente pocos documentos. Sin embargo, nuestra investigación no pudo concluir definitivamente que la persona o entidad que no estaba autorizada no accedió, usó o revelo cierta información y documentos conservados en los sistemas afectados de La Clínica, y que pueden haber incluido alguna de la siguiente información: su nombre completo, fecha de nacimiento, número de teléfono, domicilio, información del seguro de salud y cierta información de salud como fechas de servicio, diagnóstico, resultados de pruebas e información de tratamiento relacionada con la atención recibida en La Clínica. Los números de seguro social y la información de la cuenta financiera no está archivada en los sistemas afectados y por lo tanto creamos que esta información no estaba involucrada en este incidente. Además, en base a nuestras prácticas de investigación y seguridad, no tenemos ninguna razón para creer que ha habido un acceso indebido a los sistemas de facturación o registros médicos electrónicos de La Clínica.

¿Que Estamos Haciendo?

La Clinica ha tomado, y seguirá tomando, medidas para evitar que este tipo de incidente vuelva a suceder, incluye la mejoría de seguridad de nuestros datos, la implementación de salvaguardias tecnológicas adicionales incluye la detección y prevención mejoradas de intrusiones, la protección de las credenciales de acceso de sesión, la capacitación mejorada de nuestro personal y otras medidas de seguridad cibernética y otras medidas de prevención de riesgos. También hemos revisado nuestras pólizas y procedimientos de seguridad para asegurarnos de que brinden protección suficiente contra nuevos incidentes de este tipo. Además, notificamos a las autoridades federales encargadas de cumplir la ley sobre el incidente y continuaremos cooperando con su investigación.

¿Lo Que Puede Hacer Usted?

Por favor revise la sección de Información sobre Protección contra Robo de Identidad adjunta con esta carta. Esta sección describe los pasos que puede tomar para ayudar a proteger su identidad, incluidas las recomendaciones de la Comisión Federal de Comercio con respecto a la protección contra robo de identidad y detalles sobre cómo colocar una alerta de fraude o un congelamiento de seguridad en su archivo de crédito si así lo desea.

Mas información

Lamentamos profundamente cualquier preocupación o inconveniente, que este incidente pueda causarle. Tomamos muy en serio nuestra responsabilidad de proteger la información médica de nuestros pacientes. Si tiene preguntas sobre este incidente por favor llame al 855-654-0864, lunes a viernes entre 9:00 a.m. and 9:00 p.m. Hora del Pacifico.

Sincerely

Fernando Cortez
Chief Information Officer & Information Security Officer

Informacion sobre el robo de Identidad

Monitorear sus Cuentas
Nosotros recomendamos siempre revisar sus estados de cuenta y los informes crediticios. Puede obtener una copia de su informe de crédito, de cada una de las tres compañías nacionales de informe crediticio. Para solicitar su informe crediticio anual gratuito, visite www.annualcreditreport.com o por correo a Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. También comuníquese al 1-877-322-8228. La información de contacto de las tres compañías nacionales de informe crediticio aparece a continuación:

Equifax®	**Experian**	**TransUnion®**
P.O. Box 740241	P.O. Box 9701	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013-9701	Chester, PA 19016-1000
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

Cuando reciba sus informes de crédito, revíselos detenidamente. Busque cuentas o consultas de acreedores que no inició o no reconoció. Busque información, como la dirección de su casa y el número de seguro social, que no sea precisa. Si ve algo que no comprende, llame a la agencia de informes crediticios al número de teléfono que figura en el informe.

Congelamiento de Credito
Tiene derecho a colocar un congelamiento de crédito, conocido también como un congelamiento de seguridad, en su expediente crediticio, sin costo alguno, con el fin de que no se pueda abrir ningún crédito en su nombre sin usar un número de identificación personal (PIN), el cual le será expedido cuando comience un congelamiento. Un congelamiento de seguridad está diseñado para evitar que los otorgantes de crédito potenciales puedan acceder su informe de crédito sin su consentimiento. Si usted coloca un congelamiento de seguridad, los acreedores potenciales y demás terceros no podrán acceder su informe de crédito, a menos que usted retire temporalmente el congelamiento. Por lo anterior, el uso de un congelamiento de seguridad podría retrasar sus posibilidades de obtener crédito.

El colocar o retirar un congelamiento de seguridad no tiene costo alguno. A diferencia de una alerta de fraude, usted debe colocar un congelamiento de seguridad en su expediente de crédito con cada una de las compañías de reporte crediticio. Para información e instrucciones para colocar un congelamiento de crédito, comuníquese con cada una de las agencias de reporte crediticio en las siguientes direcciones:

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.equifax.com/personal/ credit-report-services	www.experian.com/ freeze/center.html	www.transunion.com/ credit-freeze

Debe colocar por separado una congelación de crédito en su archivo de crédito en cada agencia de informes crediticios. Se debe incluir la siguiente información al solicitar una congelación de crédito:

1. Nombre Completo incluyendo segundo inicial, y títulos personales como “Jr” “II”
2. Numero de Seguro Social
3. Fecha de Nacimiento (mes, día y año)
4. Dirección actual y direcciones de los últimos 5 años
5. Comprobante de domicilio actual (como recibo de teléfono o agua)
6. Otra información personal según que requiera la agencia

Si solicita una congelación de crédito en línea o por teléfono, las agencias de informes de crédito tienen un (1) día hábil después de recibir su solicitud para colocar una congelación de crédito en su informe de archivo de crédito. Si solicita un levantamiento del congelamiento de crédito en línea o por teléfono, la agencia de informes crediticios debe levantar el congelamiento dentro de una (1) hora. Si solicita una congelación de crédito o un levantamiento de una congelación de crédito por correo, entonces la agencia de crédito debe colocar o levantar la congelación de crédito a más tardar tres (3) días hábiles después de recibir su solicitud.

Alertas de Fraude
También tiene derecho a colocar una alerta de fraude inicial o extendida en su expediente sin costo alguno. Una alerta de fraude inicial dura 1 año y se coloca en el archivo de crédito del consumidor. Al ver que se muestra una alerta de fraude en el archivo de crédito de un consumidor, una empresa debe tomar medidas para verificar la identidad del consumidor antes de otorgar un nuevo crédito. Si es víctima de un robo de identidad, tiene derecho a recibir una alerta de fraude extendida, que es una alerta de fraude que dura 7 años. Si desea colocar una alerta de fraude, comuníquese con cualquiera de las agencias que se enumeran a continuación. La agencia con la que se comunique se comunicará con las otras dos agencias de crédito.

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com/personal/ credit-report-services	www.experian.com/ fraud/center.html	www.transunion.com/ fraud-victim-resource/place-fraud-alert

Monitorear su información Medica Personal

Si corresponde a su situación, le recomendamos que revise periódicamente la explicación de la declaración de beneficios que recibe de su aseguradora. Si ve algún servicio que cree que no recibió, comuníquese con su aseguradora al número que figura en el estado de cuenta. Si no recibe la explicación regular de las declaraciones de beneficios, comuníquese con su proveedor y solicítele que envíe dichas declaraciones después de la prestación de servicios en su nombre o número.

Es posible que desee solicitar copias de sus informes de crédito y verificar si hay facturas médicas que no reconozca. Si encuentra algo sospechoso, llame a la agencia de informes crediticios al número de teléfono que figura en el informe. Guarde una copia de este aviso para sus registros en caso de problemas futuros con sus registros médicos. También es posible que desee solicitar una copia de sus registros médicos a su proveedor, para que sirva como referencia. Si es residente de California, le sugerimos que visite el sitio web de la Oficina de Protección de Privacidad de California en https://oag.ca.gov/privacy/ para encontrar más información sobre cómo proteger su privacidad.

Información Adicional

Puede informarse más sobre el robo de identidad y los pasos que puede tomar para protegerse comunicándose con el Fiscal General de su estado o la Comisión Federal de Comercio. Los casos de robo de identidad conocido o sospechado deben informarse a las autoridades policiales, al Fiscal General y a la FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
https://www.ftc.gov/

La Clínica
La Clínica de La Raza, Inc.
Mailing Address: Post Office Box 22210 Oakland, CA 94623 • Tel 510-535-4000 • Fax 510-535-4189 • www.laclinica.org

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
Parent/Guardian of
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: Notice of Data Security Incident

Dear Parent/Guardian of <<Name 1>>:

This letter is to inform you of a recent data security incident that may have involved your child's personal information maintained by La Clinica de la Raza ("La Clinica"). This letter describes the incident, outlines measures that we have taken in response to the incident and provides information regarding additional steps you can take to help protect your child's information.

What Happened?

On January 28, 2021, La Clinica became aware that malware had been deployed on certain La Clinica systems which store information, including personal information, for the organization. Upon learning of the incident, La Clinica immediately took steps to stop access to these systems, including permanently disconnecting the affected systems from other La Clinica systems and its overall network. La Clinica also began an immediate investigation of the incident with the support of a third-party forensics company. On February 26, 2021, La Clinica's investigation determined that the malware was deployed by an unauthorized individual or entity who gained unauthorized access to La Clinica's systems. Upon learning of the unauthorized access, La Clinica immediately took additional mitigation steps and security measures, including deploying additional measures to monitor the organization's systems and technology infrastructure.

What Information Was Involved?

La Clinica's ongoing investigation has determined that the unauthorized access to the affected systems occurred, and ended, on January 12, 2021. Based on the investigation to date, we reasonably believe that relatively few documents were likely viewed by the unauthorized party. However, our investigation could not definitively conclude that the unauthorized party did not access, use or disclose certain information and documents stored in the affected La Clinica systems, which may have included some of the following information: your child's full name, date of birth, phone number, home address, health insurance information, and certain health information such as dates of service, diagnosis, test results, and treatment information related to care received at La Clinica. Social security numbers and financial account information were not stored in the affected systems and therefore were not involved in this incident. Further, based on our investigation and security practices, we have no reason to believe that there has been any improper access to La Clinica's electronic medical record or billing systems.

What Are We Doing?

La Clinica has taken, and will continue to take, steps to prevent this type of incident from happening again, including enhancing our data security, implementing additional technology safeguards including enhanced intrusion detection and prevention, securing login credentials, enhanced workforce training, and other cybersecurity risk prevention measures. We have also reviewed our security policies and procedures to ensure that they sufficiently protect against further incidents of this type. In addition, we notified federal law enforcement authorities about the incident and will continue to cooperate with their investigation.

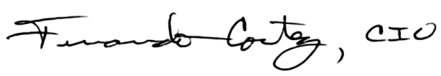
What You Can Do.

Please review the enclosed *Information About Identity Theft Protection* section included with this letter. This section describes steps you can take to help protect your child's identity, including recommendations by the Federal Trade Commission regarding identify theft protection and details on how to place a fraud alert or a security freeze on your child's credit file if you wish to do so.

For More Information.

We sincerely regret any inconvenience or concern caused by this incident. We take our responsibility to protect the personal information of our patients very seriously. If you have questions or concerns about this incident, please call 855-654-0864, Monday through Friday, between 6:00 a.m. and 6:00 p.m. Pacific Time.

Sincerely,



Fernando Cortez
Chief Information Officer & Information Security Officer

Information About Identity Theft Protection

Monitor Your Child's Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®	**Experian**	**TransUnion®**
P.O. Box 740241	P.O. Box 9701	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013-9701	Chester, PA 19016-1000
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.equifax.com/personal/ credit-report-services	www.experian.com/ freeze/center.html	www.transunion.com/ credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com/personal/ credit-report-services	www.experian.com/ fraud/center.html	www.transunion.com/ fraud-victim-resource/place-fraud-alert

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at https://oag.ca.gov/privacy/ to find more information about protecting your privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

La Clínica
La Clínica de La Raza, Inc.
Mailing Address: Post Office Box 22210 Oakland, CA 94623 • Tel 510-535-4000 • Fax 510-535-4189 • www.laclinica.org

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
Padre/Tutor de
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: Notificacion Del Incidente De Seguridad Proteccion De Datos

Estimado Padre/Tutor de <<Name 1>>:

Esta carta es para informarle de un incidente reciente de seguridad de datos que puede haber involucrado la información personal de su hijo/a mantenida por La Clínica de la Raza ("La Clínica"). Esta carta describe el incidente, describe las medidas que hemos tomado en respuesta al incidente y brinda información sobre los pasos adicionales que puede tomar para ayudar a proteger la información de su hijo/a.

¿Qué Sucedió?

El 28 de enero del 2021, La Clinica se dio cuenta que se había implementado un programa maligno (malware) en ciertos sistemas de La Clinica que guardan información, incluyendo información personal para la organización. Al enterarse del incidente, La Clinica inmediatamente tomo medidas para parar el acceso a estos sistemas, incluyendo la desconexión permanente de los sistemas afectados de otros sistemas de La Clínica y su red general. La Clínica también inició una investigación inmediata del incidente con el apoyo de una empresa forense. El 26 de febrero de 2021, la investigación de La Clínica determinó que el programa maligno (malware) fue implementado por una persona o entidad no autorizada que obtuvo acceso no autorizado a los sistemas de La Clínica. Al enterarse del acceso no autorizado, La Clínica inmediatamente tomó medidas de mitigación y medidas de seguridad adicionales, incluyendo la implementación de medidas adicionales para monitorear los sistemas y la infraestructura tecnológica de la organización.

¿Que información estuvo involucrada?

La investigación en curso de La Clinica, ha determinado que el acceso no autorizado a los sistemas afectados ocurrió y termino el 12 de enero de 2021. Basado en nuestra investigación hasta la fecha, creemos razonablemente que la persona o entidad que no estaba autorizada probablemente nomas vieron relativamente pocos documentos. Sin embargo, nuestra investigación no pudo concluir definitivamente que la persona o entidad que no estaba autorizada no accedió, usó o revelo cierta información y documentos conservados en los sistemas afectados de La Clínica, y que pueden haber incluido alguna de la siguiente información: nombre completo de su hijo, fecha de nacimiento, fecha de nacimiento, número de teléfono , domicilio, información del seguro de salud y cierta información de salud como fechas de servicio, diagnóstico, resultados de pruebas e información de tratamiento relacionada con la atención recibida en La Clínica. Los números de seguro social y la información de la cuenta financiera no está archivada en los sistemas afectados y por lo tanto creamos que esta información no estaba involucrada en este incidente. Además, en base a nuestras prácticas de investigación y seguridad, no tenemos ninguna razón para creer que ha habido un acceso indebido a los sistemas de facturación o registros médicos electrónicos de La Clínica.

¿Que Estamos Haciendo?

La Clinica ha tomado, y seguirá tomando, medidas para evitar que este tipo de incidente vuelva a suceder, incluye la mejoría de seguridad de nuestros datos, la implementación de salvaguardias tecnológicas adicionales incluye la detección y prevención mejoradas de intrusiones, la protección de las credenciales de acceso de sesión, la capacitación mejorada de nuestro personal y otras medidas de seguridad cibernética y otras medidas de prevención de riesgos. También hemos revisado nuestras pólizas y procedimientos de seguridad para asegurarnos de que brinden protección suficiente contra nuevos incidentes de este tipo. Además, notificamos a las autoridades federales encargadas de cumplir la ley sobre el incidente y continuaremos cooperando con su investigación.

¿Lo Que Puede Hacer Usted?

Por favor revise la sección de Información sobre Protección contra Robo de Identidad adjunta con esta carta. Esta sección describe los pasos que puede tomar para ayudar a proteger la identidad de su hijo, incluidas las recomendaciones de la Comisión Federal de Comercio con respecto a la protección contra el robo de identidad y detalles sobre cómo colocar una alerta de fraude o una congelación de seguridad en el archivo de crédito de su hijo si así lo desea.

Mas información

Lamentamos profundamente cualquier preocupación o inconveniente, que este incidente pueda causarle. Tomamos muy en serio nuestra responsabilidad de proteger la información médica de nuestros pacientes. Si tiene preguntas sobre este incidente por favor llame al 855-654-0864, lunes a viernes entre 6:00 a.m. and 6:00 p.m. Hora del Pacifico.

Sincerely,

Fernando Cortez
Chief Information Officer & Information Security Officer

Informacion sobre el robo de Identidad

Monitorear sus Cuentas

Nosotros recomendamos siempre revisar sus estados de cuenta y los informes crediticios. Puede obtener una copia de su informe de crédito, de cada una de las tres compañías nacionales de informe crediticio. Para solicitar su informe crediticio anual gratuito, visite www.annualcreditreport.com o por correo a Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. También comuníquese al 1-877-322-8228. La información de contacto de las tres compañías nacionales de informe crediticio aparece a continuación:

Equifax®	**Experian**	**TransUnion®**
P.O. Box 740241	P.O. Box 9701	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013-9701	Chester, PA 19016-1000
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

Cuando reciba sus informes de crédito, revíselos detenidamente. Busque cuentas o consultas de acreedores que no inició o no reconoció. Busque información, como la dirección de su casa y el número de seguro social, que no sea precisa. Si ve algo que no comprende, llame a la agencia de informes crediticios al número de teléfono que figura en el informe.

Congelamiento de Credito

Tiene derecho a colocar un congelamiento de crédito, conocido también como un congelamiento de seguridad, en su expediente crediticio, sin costo alguno, con el fin de que no se pueda abrir ningún crédito en su nombre sin usar un número de identificación personal (PIN), el cual le será expedido cuando comience un congelamiento. Un congelamiento de seguridad está diseñado para evitar que los otorgantes de crédito potenciales puedan acceder su informe de crédito sin su consentimiento. Si usted coloca un congelamiento de seguridad, los acreedores potenciales y demás terceros no podrán acceder su informe de crédito, a menos que usted retire temporalmente el congelamiento. Por lo anterior, el uso de un congelamiento de seguridad podría retrasar sus posibilidades de obtener crédito.

El colocar o retirar un congelamiento de seguridad no tiene costo alguno. A diferencia de una alerta de fraude, usted debe colocar un congelamiento de seguridad en su expediente de crédito con cada una de las compañías de reporte crediticio. Para información e instrucciones para colocar un congelamiento de crédito, comuníquese con cada una de las agencias de reporte crediticio en las siguientes direcciones:

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.equifax.com/personal/ credit-report-services	www.experian.com/ freeze/center.html	www.transunion.com/ credit-freeze

Debe colocar por separado una congelación de crédito en su archivo de crédito en cada agencia de informes crediticios. Se debe incluir la siguiente información al solicitar una congelación de crédito:

1. Nombre Completo incluyendo segundo inicial, y títulos personales como “Jr” “II”
2. Numero de Seguro Social
3. Fecha de Nacimiento (mes, día y año)
4. Dirección actual y direcciones de los últimos 5 años
5. Comprobante de domicilio actual (como recibo de teléfono o agua)
6. Otra información personal según que requiera la agencia

Si solicita una congelación de crédito en línea o por teléfono, las agencias de informes de crédito tienen un (1) día hábil después de recibir su solicitud para colocar una congelación de crédito en su informe de archivo de crédito. Si solicita un levantamiento del congelamiento de crédito en línea o por teléfono, la agencia de informes crediticios debe levantar el congelamiento dentro de una (1) hora. Si solicita una congelación de crédito o un levantamiento de una congelación de crédito por correo, entonces la agencia de crédito debe colocar o levantar la congelación de crédito a más tardar tres (3) días hábiles después de recibir su solicitud.

Alertas de Fraude

También tiene derecho a colocar una alerta de fraude inicial o extendida en su expediente sin costo alguno. Una alerta de fraude inicial dura 1 año y se coloca en el archivo de crédito del consumidor. Al ver que se muestra una alerta de fraude en el archivo de crédito de un consumidor, una empresa debe tomar medidas para verificar la identidad del consumidor antes de otorgar un nuevo crédito. Si es víctima de un robo de identidad, tiene derecho a recibir una alerta de fraude extendida, que es una alerta de fraude que dura 7 años. Si desea colocar una alerta de fraude, comuníquese con cualquiera de las agencias que se enumeran a continuación. La agencia con la que se comunique se comunicará con las otras dos agencias de crédito.

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com/personal/credit-report-services	www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert

Monitorear su información Medica Personal

Si corresponde a su situación, le recomendamos que revise periódicamente la explicación de la declaración de beneficios que recibe de su aseguradora. Si ve algún servicio que cree que no recibió, comuníquese con su aseguradora al número que figura en el estado de cuenta. Si no recibe la explicación regular de las declaraciones de beneficios, comuníquese con su proveedor y solicítele que envíe dichas declaraciones después de la prestación de servicios en su nombre o número.

Es posible que desee solicitar copias de sus informes de crédito y verificar si hay facturas médicas que no reconozca. Si encuentra algo sospechoso, llame a la agencia de informes crediticios al número de teléfono que figura en el informe. Guarde una copia de este aviso para sus registros en caso de problemas futuros con sus registros médicos. También es posible que desee solicitar una copia de sus registros médicos a su proveedor, para que sirva como referencia. Si es residente de California, le sugerimos que visite el sitio web de la Oficina de Protección de Privacidad de California en https://oag.ca.gov/privacy/para encontrar más información sobre cómo proteger su privacidad.

Información Adicional

Puede informarse más sobre el robo de identidad y los pasos que puede tomar para protegerse comunicándose con el Fiscal General de su estado o la Comisión Federal de Comercio. Los casos de robo de identidad conocido o sospechado deben informarse a las autoridades policiales, al Fiscal General y a la FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261