LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, TX 75201
Lindsay.Nickle@LewisBrisbois.com
214.722.7141

April 30, 2019

VIA E-MAIL
Attorney General Wayne Stenehjem
Office of the Attorney General
Consumer Protection and Antitrust
1050 East Interstate Avenue, Suite 200
Bismarck, ND 58503-5574
Email: ndag@nd.gov

Re: Notification of Data Security Incident

Dear Attorney General Stenehjem:

I represent Inmediata Health Group, Corp., ("Inmediata") located in San Juan, Puerto Rico, with respect to a recent data security incident described in greater detail below. Inmediata is taking steps to prevent similar incidents from occurring in the future.

1. **Nature of the security incident.**

In January 2019, Inmediata became aware that some of its customers' patients' electronic protected health information (PHI) was publicly available online as a result of a webpage setting that permitted search engines to index pages that are part of an internal website Inmediata uses for business operations. Upon discovering the incident, Inmediata immediately deactivated the website and engaged an independent computer forensics firm to assist with analysis. Based on the investigation, Inmediata has no evidence that any files were copied or saved or that the data has been misused. Additionally, no financial information was involved. The information has been delisted from online search engines and the authentication setting for the webpage has been fixed.

Although there is no evidence that any PHI has been acquired or misused, Inmediata is in the process of notifying the potentially affected population. The information involved includes patients' names, addresses, dates of birth, gender, and medical claim information, including dates of service, diagnosis codes, procedure codes, and treating physician. In addition, for a very small subset of the population Inmediata is notifying, Social Security numbers may have been impacted.

2. Number of North Dakota residents notified.

A total of 685 residents of North Dakota were potentially affected by this incident. On April 22, 2019, Inmediata began notifying the involved North Dakota residents via the enclosed letter, which was sent by direct mail.

3. Steps taken relating to the incident.

Inmediata has taken steps in response to this incident to strengthen the security of personal information in its possession. In addition to repairs to the authentication for the involved website, Inmediata is conducting system-wide assessments of its network to ensure that all information Inmediata collects, stores, and uses is secure. Inmediata is continuing to implement additional security measures and is committed to protecting the security and integrity of all of information in its systems.

In addition, for those patients whose Social Security numbers are involved, Inmediata is offering twelve months of complimentary identity protection and credit monitoring services at no cost to the patient.

4. Contact information.

Inmediata remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (214) 722-7141 or by e-mail at lindsay.nickle@lewisbrisbois.com.

Please let me know if you have any questions

Very truly yours,

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Consumer Notification Letter

Seibel, Jessica K.

From: Nickle, Lindsay <Lindsay.Nickle@lewisbrisbois.com>
Sent: Wednesday, May 1, 2019 12:10 AM
To: -Info-Attorney General
Cc: Nair, Bindu; Nickle, Lindsay
Subject: Inmediata: Notification of Data Security Incident (ND)
Attachments: Inmediata -- AG (North Dakota).pdf

CAUTION: This email originated from an outside source. Do not click links or open attachments unless you know they are safe.

Please see the attached correspondence being sent on behalf of my client, Inmediata Health Group, Corp.

If there are any questions, please let me know.

Best regards,
Lindsay Nickle

Lindsay B. Nickle
Partner
Lindsay.Nickle@lewisbrisbois.com

T: 214.722.7141 F: 214.722.7111

2100 Ross Avenue, Suite 2000, Dallas, Texas 75201 | **LewisBrisbois.com**

Representing clients from coast to coast. View our locations nationwide.

This e-mail may contain or attach privileged, confidential or protected information intended only for the use of the intended recipient. If you are not the intended recipient, any review or use of it is strictly prohibited. If you have received this e-mail in error, you are required to notify the sender, then delete this email and any attachment from your computer and any of your electronic devices where the message is stored.

INMEDIATA
Services you trust for health.

April 22, 2019

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Security Incident

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

I am writing on behalf of Inmediata Health Group, Corp., (Inmediata) to inform you of a data security incident that may have resulted in the potential disclosure of your personal and medical information. At Inmediata, we take the security of all patient information very seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains information about steps you can take to protect your information and resources we are making available to you.

What Happened?

In January 2019, Inmediata became aware that some of its member patients' electronic patient health information was publicly available online as a result of a webpage setting that permitted search engines to index pages that are part of an internal website we use for our business operations. When we became aware of the incident, we immediately deactivated the website and engaged an independent computer forensics firm to assist us. Based on the investigation, we have no evidence that any files were copied or saved. In addition, we have not discovered any evidence that any information that may be involved in this incident has been misused. However, out of an abundance of caution, we are informing you about the incident and providing you with information and resources to assist you.

What information was involved?

The information potentially impacted by this incident may have included your name, address, date of birth, gender, and medical claim information including dates of service, diagnosis codes, procedure codes and treating physician. Please note that neither your Social Security number nor your financial information is involved in this incident.

What We Are Doing.

As soon as we learned about the incident, we took the steps described above. In addition, we are providing you with information about steps you can take to help protect your personal information. Also, we have taken steps to remove any indexed information from public search engines, and we are conducting system-wide assessments to ensure that our system and the information we store is secure.

What You Can Do.

As stated above, while we are not aware of the misuse of any information potentially involved in this incident, you can follow the recommendations included with this letter to protect your personal information.

For more information.

We sincerely regret any inconvenience or concern that this matter may cause you and remain dedicated to protecting all information in our systems. Please do not hesitate to call 1-833-389-2392, Monday through Friday, 9:00 a.m. to 6:30 p.m. Eastern Time if you have questions about this event.

Sincerely,

Mark Rieger
CEO
Inmediata

9303AF-0419

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

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

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

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file. 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 steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

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

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

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

INMEDIATA
Services you trust for health.

April 22, 2019

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Security Incident

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

I am writing on behalf of Inmediata Health Group, Corp., (Inmediata) to inform you of a data security incident that may have resulted in the potential disclosure of your personal and medical information. At Inmediata, we take the security of all patient information very seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains information about steps you can take to protect yourself and resources we are making available to you.

What Happened?

In January 2019, Inmediata became aware that some individuals' electronic patient health information was available online because of a webpage setting that permitted search engines to index pages that are part of an internal website we use for our business operations. When we became aware of the incident, we immediately deactivated the website and engaged an independent computer forensics firm to assist us. Based on the investigation, we have no evidence that any files were copied or saved. In addition, we have discovered no evidence that any information that may be involved in this incident has been misused. However, out of an abundance of caution, we are informing you about the incident and providing you with information and resources to assist you.

What information was involved?

The information potentially impacted by this incident may have included your name, address, Social Security number, date of birth, gender, and medical claim information, including dates of service, diagnosis codes, procedure codes and treating physician. Please note that your financial information is not involved in this incident.

What We Are Doing.

As soon as we learned about the incident, we took the steps described above. In addition, we are providing you with information about steps you can take to help protect your personal information. We also have taken steps to remove any indexed information from public search engines, and we are conducting system-wide assessments to ensure that our system and the information we store is secure.

What You Can Do.

While we do not believe any patient personal information was at risk, you can follow the recommendations included with this letter to protect your personal information. In addition, as a precautionary measure to safeguard your information from potential misuse, we are offering identity monitoring services for one year at no cost to you through Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until **July 31, 2019** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-833-389-2392. Additional information describing your services is included with this letter.

If you have questions or concerns about possible fraud, please call 1-833-389-2392, Monday through Friday, 9:00 a.m. to 6:30 p.m. Eastern Time.

For more information.

We sincerely regret any inconvenience or concern that this matter may cause you and remain dedicated to protecting all information in our systems. Please do not hesitate to call 1-833-389-2392, Monday through Friday, 9:00 a.m. to 6:30 p.m. Eastern Time if you have questions about this event.

Sincerely,

Mark Rieger
CEO
Inmediata

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

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

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

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file. 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 steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

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

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

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

Kroll. | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

INMEDIATA
Services you trust for health.

22 de abril de 2019

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Asunto: Notificación de Incidente de Seguridad

Estimado/a <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Escribo a nombre de Inmediata Health Group Corp (Inmediata) para informarles de un incidente de seguridad de datos que pudo haber resultado en divulgación de su información personal y médica. En Inmediata, tomamos en serio la seguridad de la información de pacientes, y pido disculpas por cualquier inconveniente que este incidente pueda causar. Esta carta contiene información sobre los pasos que usted puede seguir para proteger la información, y brindamos los recursos que ponemos a su disposición.

¿Qué ocurrió?

En enero de 2019, Inmediata se percató que información electrónica sobre la salud de los pacientes de algunos miembros, estaba disponible en línea públicamente como resultado de una configuración de página web que permitía a los mecanismos de búsqueda indexar páginas que pertenecen a un sitio web interno que utilizamos en las operaciones comerciales. Inmediatamente reportado el incidente, desactivamos el sitio web y contratamos una entidad independiente, expertos en informática forense para asistirnos. Basados en los hallazgos de la investigación, no tenemos evidencia que algún archivo fuese copiado o guardado. En adición, no hemos descubierto evidencia alguna que susodicha información ha sido mal utilizada. Sin embargo, tomando todas las precauciones, le informamos sobre el incidente, proveemos la información y recursos para asistirle.

¿Qué información estaba involucrada?

La información que potencialmente esta involucrada en este incidente, puede que incluya: su nombre, dirección, fecha de nacimiento, sexo, e información sobre reclamaciones médicas, incluidas las fechas de servicio, códigos de diagnóstico, códigos de procedimiento y médico que le atendió. Le informamos que ni su número de seguro social, tampoco su información financiera esta incluida en el incidente.

¿Qué estamos haciendo?

Tan pronto como nos enteramos del incidente, seguimos los pasos descritos anteriormente. Además, le proporcionamos información sobre los pasos que puede seguir para ayudar a proteger su información personal. Conjuntamente, hemos tomado medidas para eliminar cualquier información indexada de los mecanismos de búsqueda públicos, y estamos realizando evaluaciones de todos nuestros sistemas informáticos para asegurar que dichos sistemas y la información que almacenamos estén seguros.

¿Qué puede hacer usted?

Como se indica anteriormente, sabiendo que no hemos descubierto evidencia alguna que la información potencialmente involucrada en el incidente ha sido mal utilizada, puede seguir las recomendaciones incluidas en esta carta para proteger su información personal.

Para más información

Lamentamos sinceramente cualquier inconveniente o inquietud que este asunto pueda causarle mientras nosotros nos mantenemos dedicados a proteger toda la información en nuestros sistemas. No dude en llamar al 1-833-389-2392 de lunes a viernes, de 9:00 - 6:30 pm AST.

Sinceramente,

Mark Rieger
CEO
Inmediata Health Group Corp.

9303AI-0419

PASOS QUE PUEDE SEGUIR PARA PROTEGER SU INFORMACIÓN

Revise sus estados de cuenta y notifique a la Autoridades Policiacas actividades sospechosas: Como medida de precaución, le recomendamos que permanezca atento revisando sus estados de cuenta e informes de crédito detenidamente. Si detecta cualquier actividad sospechosa en una cuenta, debe notificar de inmediato a la institución financiera o compañía con la que se mantiene la cuenta. También debe informar con prontitud cualquier actividad fraudulenta o sospecha de incidencia de robo de identidad a las autoridades policiales adecuadas, al fiscal general de su estado y/o a la "Federal Trade Commission" (FTC).

Copia del informe de crédito: Puede obtener una copia gratuita de su informe de crédito de cada una de las tres principales agencias de informes de crédito una vez cada 12 meses visitando http://www.annualcreditreport.com , llamando al número gratuito 877-322-8228 , o al completar un Formulario de solicitud de informe de crédito anual y enviarlo por correo al Servicio de solicitud de informe de crédito anual, PO Box 105281, Atlanta, GA 30348. Puede imprimir este formulario en https://www.annualcreditreport.com/cra/requestformfinal.pdf . También puede comunicarse con una de las siguientes tres agencias nacionales de informes de crédito:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Alerta de 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 al menos 90 días. 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: http://www.annualcreditreport.com

Congelamiento de Seguridad: Usted tiene el derecho de poner un congelamiento de seguridad en su expediente de crédito. Esto evitará que se abra un nuevo crédito a su nombre sin el uso de un número de PIN que se le emite la agencia de informe crediticio al iniciar la congelación. El congelamiento de seguridad está diseñado para evitar que los acreedores potenciales tengan acceso a su informe de crédito sin su consentimiento. Como resultado, el uso de una congelación de seguridad puede interferir o retrasar su capacidad para obtener crédito. Debe notificar por separado en su archivo de crédito con cada agencia de informes de crédito. Es posible que deba proporcionar la agencia de información con la información que lo identifica a usted, incluyendo su nombre completo, número de seguro social, fecha de nacimiento, dirección actual y anterior, una copia de su tarjeta de identificación emitida por el estado y una declaración reciente factura de servicios públicos, estado de cuenta bancario o seguro.

Recursos gratuitos adicionales: Puede obtener información de las agencias de informes de consumidores, la FTC o de su respectivo Fiscal General del estado sobre los pasos que puede tomar para prevenir el robo de identidad. Puede denunciar sospechas de robo de identidad a las autoridades locales, incluso a la FTC o al Fiscal General en su estado. Los residentes de Maryland, Carolina del Norte y Rhode Island pueden obtener más información de sus Fiscales Generales utilizando la información de contacto a continuación.

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

También tiene ciertos derechos bajo la Ley de "Fair Credit Reporting Act" (FCRA, por sus siglas en inglés), incluido el derecho a saber qué hay en su archivo, a disputar información incompleta o inexacta, y a las agencias de informes de consumidores a corregir o eliminar información inexacta, incompleta o no verificable. Para obtener más información sobre la FCRA y sus derechos de conformidad con la FCRA, visite http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf

Información personal de un menor de edad: 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. Pueden requerirse copias de la información de identificación para el menor y el padre / tutor, incluyendo el certificado de nacimiento o adopción, la tarjeta de Seguro Social y la tarjeta de identificación emitida por el gobierno. Si existe un informe de crédito, debe solicitar una copia del informe e inmediatamente reportar cualquier cuenta fraudulenta a la agencia de informes de crédito. También puede reportar cualquier uso indebido de la información del menor a la FTC en https://www.identitytheft.gov/. Para obtener más información sobre el robo de identidad infantil y las instrucciones para solicitar una búsqueda manual del número de Seguro Social, visite el sitio web https://www.consumer.ftc.gov/articles/0040-child-identity-theft.

INMEDIATA
Services you trust for health.

22 de abril de 2019

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Asunto: Notificación de Incidente de Seguridad

Estimado/a <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Escribo a nombre de Inmediata Health Group Corp (Inmediata) para informarles de un incidente de seguridad de datos que pudo haber resultado en divulgación de su información personal y médica. En Inmediata, tomamos en serio la seguridad de la información de pacientes, y pido disculpas por cualquier inconveniente que este incidente pueda causar. Esta carta contiene información sobre los pasos que usted puede seguir para proteger la información, y brindamos los recursos que ponemos a su disposición.

¿Qué ocurrió?

En enero de 2019, Inmediata se percató que información electrónica sobre la salud de los pacientes de algunos miembros, estaba disponible en línea públicamente en línea como resultado de una configuración de página web que permitía a los mecanismos de búsqueda indexar páginas que pertenecen a un sitio web interno que utilizamos en las operaciones comerciales. Inmediatamente reportado el incidente, desactivamos el sitio web y contratamos una entidad independiente, expertos en informática forense para asistirnos. Basados en los hallazgos de la investigación, no tenemos evidencia que algún archivo fuese copiado o guardado. En adición, no hemos descubierto evidencia alguna que susodicha información ha sido mal utilizada. Sin embargo, tomando todas las precauciones, le informamos sobre el incidente, proveemos la información y recursos para asistirle.

¿Qué información estaba involucrada?

La información que potencialmente esta involucrada en este incidente, puede que incluya: su nombre, dirección, número de Seguro Social, fecha de nacimiento, sexo, e información sobre reclamaciones médicas, incluidas las fechas de servicio, códigos de diagnóstico, códigos de procedimiento y médico que le atendió. Le informamos que su información financiera no está incluida en el incidente.

¿Qué estamos haciendo?

Tan pronto como nos enteramos del incidente, seguimos los pasos descritos anteriormente. Además, le proporcionamos información sobre los pasos que puede seguir para ayudar a proteger su información personal. Conjuntamente, hemos tomado medidas para eliminar cualquier información indexada de los mecanismos de búsqueda públicos, y estamos realizando evaluaciones de todos nuestros sistemas informáticos para asegurar que dichos sistemas y la información que almacenamos estén seguros.

¿Qué puede hacer usted?

Como se indica anteriormente, sabiendo que no hemos descubierto evidencia alguna que la información potencialmente involucrada en el incidente ha sido mal utilizada, puede seguir las recomendaciones incluidas en esta carta para proteger su información personal. Además, como medida de precaución para proteger su información de posible uso indebido, estamos ofreciendo servicios de monitoreo de identidad por un año sin costo alguno para usted a través de Kroll. Kroll es un líder global en la mitigación y respuesta a los riesgos, y su equipo tiene una amplia experiencia ayudando a las personas que hayan sufrido una exposición no intencional de datos confidenciales. Sus servicios de monitoreo de identidad incluyen Monitoreo de crédito, Consulta de fraude y Restauración de robo de identidad.

Visite **my.idmonitoringservice.com** para activar y beneficiarse de los servicios de monitoreo de identidad.

Usted tendrá hasta ***July 31, 2019*** para activar los servicios de monitoreo.

Su numero de Miembro es: <<Member ID>>

Para recibir servicios de monitoreo de crédito por correo en ves de en línea, favor llamar al 1-833-389-2392. Información adicional describiendo estos servicios está incluido en este comunicado.

De tener dudas o preguntas sobre posible fraude, favor llamar 1-833-389-2392, lunes a viernes, 9:00 - 6:30 pm EST.

Para más información

Lamentamos sinceramente cualquier inconveniente o inquietud que este asunto pueda causarle mientras nosotros nos mantenemos dedicados a proteger toda la información en nuestros sistemas. No dude en llamar al 1-833-389-2392 de lunes a viernes, de 9:00 - 6:30 pm AST.

Sinceramente,

Mark Rieger
CEO
Inmediata Health Group Corp.

PASOS QUE PUEDE SEGUIR PARA PROTEGER SU INFORMACIÓN

Revise sus estados de cuenta y notifique a la Autoridades Policiacas actividades sospechosas: Como medida de precaución, le recomendamos que permanezca atento revisando sus estados de cuenta e informes de crédito detenidamente. Si detecta cualquier actividad sospechosa en una cuenta, debe notificar de inmediato a la institución financiera o compañía con la que se mantiene la cuenta. También debe informar con prontitud cualquier actividad fraudulenta o sospecha de incidencia de robo de identidad a las autoridades policiales adecuadas, al fiscal general de su estado y/o a la "Federal Trade Commission" (FTC).

Copia del informe de crédito: Puede obtener una copia gratuita de su informe de crédito de cada una de las tres principales agencias de informes de crédito una vez cada 12 meses visitando http://www.annualcreditreport.com , llamando al número gratuito 877-322-8228 , o al completar un Formulario de solicitud de informe de crédito anual y enviarlo por correo al Servicio de solicitud de informe de crédito anual, PO Box 105281, Atlanta, GA 30348. Puede imprimir este formulario en https://www.annualcreditreport.com/cra/requestformfinal.pdf . También puede comunicarse con una de las siguientes tres agencias nacionales de informes de crédito:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Alerta de 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 al menos 90 días. 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: http://www.annualcreditreport.com

Congelamiento de Seguridad: Usted tiene el derecho de poner un congelamiento de seguridad en su expediente de crédito. Esto evitará que se abra un nuevo crédito a su nombre sin el uso de un número de PIN que se le emite la agencia de informe crediticio al iniciar la congelación. El congelamiento de seguridad está diseñado para evitar que los acreedores potenciales tengan acceso a su informe de crédito sin su consentimiento. Como resultado, el uso de una congelación de seguridad puede interferir o retrasar su capacidad para obtener crédito. Debe notificar por separado en su archivo de crédito con cada agencia de informes de crédito. Es posible que deba proporcionar la agencia de información con la información que lo identifica a usted, incluyendo su nombre completo, número de seguro social, fecha de nacimiento, dirección actual y anterior, una copia de su tarjeta de identificación emitida por el estado y una declaración reciente factura de servicios públicos, estado de cuenta bancario o seguro.

Recursos gratuitos adicionales: Puede obtener información de las agencias de informes de consumidores, la FTC o de su respectivo Fiscal General del estado sobre los pasos que puede tomar para prevenir el robo de identidad. Puede denunciar sospechas de robo de identidad a las autoridades locales, incluso a la FTC o al Fiscal General en su estado. Los residentes de Maryland, Carolina del Norte y Rhode Island pueden obtener más información de sus Fiscales Generales utilizando la información de contacto a continuación.

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

También tiene ciertos derechos bajo la Ley de "Fair Credit Reporting Act" (FCRA, por sus siglas en inglés), incluido el derecho a saber qué hay en su archivo, a disputar información incompleta o inexacta, y a las agencias de informes de consumidores a corregir o eliminar información inexacta, incompleta o no verificable. Para obtener más información sobre la FCRA y sus derechos de conformidad con la FCRA, visite http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf

Información personal de un menor de edad: 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. Pueden requerirse copias de la información de identificación para el menor y el padre / tutor, incluyendo el certificado de nacimiento o adopción, la tarjeta de Seguro Social y la tarjeta de identificación emitida por el gobierno. Si existe un informe de crédito, debe solicitar una copia del informe e inmediatamente reportar cualquier cuenta fraudulenta a la agencia de informes de crédito. También puede reportar cualquier uso indebido de la información del menor a la FTC en https://www.identitytheft.gov/. Para obtener más información sobre el robo de identidad infantil y las instrucciones para solicitar una búsqueda manual del número de Seguro Social, visite el sitio web https://www.consumer.ftc.gov/articles/0040-child-identity-theft.

Kroll. | A Division of DUFF&PHELPS

Aproveche Los Servicios De Monitoreo De Su Identidad

Se le ha brindado acceso a los siguientes servicios[1] de Kroll:

Bureau único de Monitoreo de crédito

Recibirá alertas cuando haya cambios en su información crediticia, por ejemplo --- cuando se solicite una nueva línea de crédito bajo su identidad, si no reconoce la actividad, tendrá la opción de llamar a un especialista en fraude de Kroll, quien le asistirá a determinar si es un indicador de robo de identidad.

Consulta de fraude

Usted tiene acceso ilimitado a la consulta con un especialista en fraude de Kroll. El apoyo incluye mostrarle las formas más efectivas de proteger su identidad, explicando sus derechos y protecciones conforme a la ley, asistencia con alertas de fraude e interpretar cómo se accede y utiliza la información personal. Se incluye la investigación de actividades sospechosas que podrían estar vinculadas a un evento de robo de identidad.

Restauración por robo de identidad

Si se convierte en víctima de un robo de identidad, un investigador experimentado con licencia de Kroll trabajará para resolver los problemas relacionados. Tendrá acceso a un investigador dedicado que comprende sus problemas y puede hacer la mayor parte del trabajo por usted. Su investigador puede profundizar para descubrir el alcance del robo de identidad y luego trabajar para resolverlo.

[1] el sitio web de activación de Kroll solo es compatible con la versión actual o una versión anterior de Internet Explorer, Chrome, Firefox y Safari. Para recibir servicios de crédito, debe ser mayor de 18 años y tener un crédito establecido en los EE. UU. o sus territorios, tener un número de Seguro Social a su nombre y una dirección residencial de los EE. UU o sus territorios asociada con su archivo de crédito.