OPEN DOOR
FAMILY MEDICAL CENTER

19312

Return Mail Processing Center
PO 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: <<<<Variable data 3>>>>. Please read this entire letter.

Dear <<Name 1 >>,

For almost fifty years, Open Door Family Medical Center has remained committed to keeping our communities healthy. Your trust is so important to us, and we take the privacy and safety of our patients very seriously. That is why I am writing to inform you of a data security incident recently experienced by Open Door. In addition to informing you of the incident, I would like to share the steps we are taking, and the resources we are making available.

What Happened:

On August 26, 2020, Open Door experienced a ransomware event that blocked access to our computer systems. We immediately took steps to ensure no further impact, while also restoring the impacted systems. We added additional security measures and began a cybersecurity investigation with expert consultants. The investigation found that Open Door data, which may include patient information, was potentially subject to unauthorized access.

What Information Was Involved:

The personal information that may have been viewed by the unauthorized individual(s) may have included your name, in combination with: <<data elements>>.

What We Are Doing:

We have taken the necessary steps to address the incident and we are committed to protecting patient information. When we learned of this incident, we immediately locked down our network, and began to restore the impacted systems; we secured the environment to help prevent similar incidents from occurring in the future. Additionally, we updated our internal procedures and retained a third-party forensic firm to conduct a thorough investigation.

Credit Monitoring:

For your peace of mind, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<12/24>> months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. Due to privacy laws, you must enroll directly. Information regarding how to enroll in the complimentary credit monitoring service is enclosed.

What You Can Do:

Although we do not believe any personally identifiable information has been viewed or misused, you may choose to enroll in the complimentary credit monitoring service. We also recommend reviewing your accounts and being aware of any unusual activity. You may have questions or need additional information, so please feel free to contact 855-914-4698.

I want to personally express my deepest regret for any worry or inconvenience that this incident may cause you. Our patients are Open Door's top priority, and we will remain committed to supporting you and your family, now and in the future.

Sincerely,

Lindsay Farrell
President & CEO, Open Door Family Medical Center

OPEN DOOR
FAMILY MEDICAL CENTER

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

7 de Diciembre de 2020

RE: <<Variable data 3>>. Por favor lea esta carta completa.

Estimado/a << Name 1 >>,

Durante casi cincuenta años, Open Door Family Medical Center ha mantenido su compromiso de mantener saludables a nuestras comunidades. Su confianza es muy importante para nosotros y tomamos muy en serio la privacidad y seguridad de nuestros pacientes. Es por eso que le escribo para informarle de un incidente de seguridad de datos que Open Door tuvo recientemente. Además de informarles del incidente, me gustaría compartirles los pasos que estamos tomando y los recursos que estamos poniendo a disposición.

Que pasó:

El 26 de agosto de 2020, Open Door atravesó un evento de "ransomware" (un secuestro de datos) que bloqueó el acceso a nuestros sistemas informáticos. Inmediatamente tomamos medidas para garantizar que no hubiera más impacto, al mismo tiempo que restauramos los sistemas afectados. Agregamos medidas de seguridad adicionales y comenzamos una investigación de ciberseguridad con consultores expertos. La investigación encontró que los datos de Open Door, que pueden incluir información del paciente, estaban potencialmente sujetos a acceso no autorizado.

Qué información estuvo involucrada:

La información personal que puede haber sido vista por personas no autorizadas puede haber incluido su nombre, en combinación con: <<data elements>>.

Qué estamos haciendo:

Hemos tomado las medidas necesarias para abordar el incidente y estamos comprometidos a proteger la información de pacientes. Cuando nos enteramos de este incidente, inmediatamente bloqueamos nuestra red y comenzamos a restaurar los sistemas afectados. Aseguramos el ambiente para ayudar a evitar que ocurran incidentes similares en el futuro. Además, actualizamos nuestros procedimientos internos y contratamos a una firma forense externa para realizar una investigación completa.

Monitoreo de crédito:

Para su tranquilidad, hemos hecho arreglos para que se inscriba, sin ningún costo para usted, en un servicio de monitoreo de crédito en línea (myTrueIdentity) por << 12/24 >> meses, proporcionado por *TransUnion Interactive*, una subsidiaria de TransUnion®, una de las tres empresas nacionales de informes de crédito. Debido a las leyes de privacidad, usted debe inscribirse directamente. Se adjunta información sobre cómo inscribirse en el servicio gratuito de supervisión de crédito.

Lo que puede hacer:

Aunque no creemos que se haya visto o utilizado indebidamente ninguna información de identificación personal, puede optar por inscribirse en el servicio gratuito de supervisión de crédito. También recomendamos revisar sus cuentas y estar al tanto de cualquier actividad inusual. Es posible que tenga preguntas o necesite información adicional, así que no dude en comunicarse al 855-914-4698.

Quiero expresar personalmente mis más profundas disculpas por cualquier preocupación o inconveniente que este incidente pueda causarle. Nuestros pacientes son la prioridad principal de Open Door y seguiremos comprometidos a apoyarle a usted y a su familia, ahora y en el futuro.

Sinceramente,

Lindsay Farrell
Presidenta y Directora Ejecutivo, Open Door Family Medical Center

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

TransUnion® *my*TrueIdentity provides you with the following key features:

- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- <<12/24>> months of unlimited access to your TransUnion® credit report and credit score.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible.[1]

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<< Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Engagement Number>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

➢ PLACE A 1-YEAR FRAUD ALERT ON YOUR CREDIT FILE

An **initial 1-year security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request when a fraud alert is active. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

TransUnion
Fraud Victim Assistance Dept.
P.O. Box 6790
Fullerton, CA 92834
1-800-680-8289
www.transunion.com

Experian
National Consumer Assistance
P.O. Box 1017
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax
Consumer Fraud Division
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

➢ PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies. You should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. The process to place a security freeze requires that you directly contact each of the credit reporting companies. You can do so online or through the mail. The necessary types of information include your full name, social security number, date of birth, current address, all addresses where you have lived during the last two years, email address, a copy of a utility bill, bank or insurance statement and a copy of a government-issued id card, such as a driver's license or state id card.

➢ ORDER YOUR FREE ANNUAL CREDIT REPORTS

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. Visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➢ MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

[1] (Policy limitations and exclusions may apply.)

➢ USE TOOLS FROM CREDIT PROVIDERS

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

➢ BE AWARE OF SUSPICIOUS ACTIVITY INVOLVING YOUR HEALTH INSURANCE

Contact your healthcare provider if bills do not arrive when expected, and review your Explanation of Benefit forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

➢ RIGHTS UNDER THE FAIR CREDIT REPORTING ACT (FCRA)

You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to your employees; (v) you may limit "prescreened" offers of credit an insurance you get based on information in your credit report; (vi) and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

➢ OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. Additionally, any suspected identity theft should be reported to law enforcement, including your state Attorney General and the Federal Trade Commission. Additional information is available at http://www.annualcreditreport.com. Under Rhode Island and Massachusetts law, you have the right to obtain any police report filed in regard to this incident.

- Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.

- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft. For Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.

- **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

- **For New York residents,** you may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotectionl; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

- **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

- **For Rhode Island Residents,** the Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov or 401-274-4400.