Verity Medical Foundation
400 Race Street, San Jose, CA 95126

March 11, 2019

[redacted]

RE: Notice of Possible Data Breach

Dear [redacted]:

Verity Medical Foundation ("VMF" or "Foundation") takes the privacy and security of all of the personal information it maintains very seriously. We are writing to inform you that, unfortunately, it is possible that the security of your information may have been compromised as a result of the unauthorized activity of a third party.

What Happened?
On January 16, 2019, the Microsoft 365 web email account of a VMF employee was compromised for several hours. During this time, a third party obtained access to the employee's email account without authorization and from this account, sent emails to various internal and external email accounts containing a malicious link. It appears that this was an attempt to obtain user names and passwords from the recipients of these emails. We have confirmed that the third party did not gain access to the email accounts of any other VMF employee or to the VMF servers or network more generally.

During the window when the VMF employee's email account was accessed by an unauthorized third party, the intruder had the ability to access any emails or attachments present in any of the employee's email folders at the time. We reviewed the employee's email folders and have determined that one or more of the email attachments included some of your personal information from encounters with Verity Medical Foundation or its affiliated and/or contracted medical groups or physicians.

We have not been able to conclude whether the third party actually accessed, viewed or read your personal information. More importantly, your information does not appear to have been sent or forwarded and to date, we are not aware of any misuse of your information. Out of an abundance of caution, we wanted to let you know about this incident and notify you of options available to you to protect yourself.

What Information Was Involved?
The emails and attachments containing personal information that may have been accessed without authorization included names, dates of birth, patient identification numbers, phone numbers, addresses, name of health plans, health insurance policy numbers, subscriber identification numbers, unique health insurance identifiers, application and claims history, social security numbers, and driver's licenses. The

Verity Medical Foundation
400 Race Street, San Jose, CA 95126

March 11, 2019

[redacted]

Asunto: Notificación de posible filtración de datos

Estimado/a [redacted]:

Verity Medical Foundation ("VMF" o la "Fundación") se toma muy en serio los asuntos relacionados con la privacidad y la seguridad de toda la información personal que guarda. Nos comunicamos con usted para informarle que, desafortunadamente, es posible que la seguridad de sus datos se haya visto comprometida como resultado de una actividad no autorizada de un tercero.

¿Qué sucedió?
El 16 de enero de 2019, la cuenta de correo electrónico de Microsoft 365 de un empleado de VMF se vio comprometida por varias horas. Durante ese período, un tercero obtuvo acceso a la cuenta de correo electrónico del empleado sin autorización y, desde esa cuenta, envió correos electrónicos que contenían un enlace malicioso a diferentes cuentas, tanto internas como externas. Al parecer, este acto fue un intento de obtener nombres y contraseñas de los usuarios que recibieron estos correos electrónicos. Hemos confirmado que el tercero no obtuvo acceso a las cuentas de correo electrónico de ningún otro empleado de VMF, así como tampoco a los servidores ni a la red de VMF en términos más generales.

Durante el período en el que se accedió a la cuenta de correo electrónico del empleado de VMF sin autorización, el intruso tuvo la capacidad de acceder a cualquier correo electrónico y archivos adjuntos presentes hasta ese momento en las carpetas de la cuenta del empleado. Revisamos las carpetas de correo electrónico y hemos determinado que uno o más de los archivos adjuntos incluía información personal sobre usted recopilada de sus encuentros con Verify Medical Foundation o sus médicos o grupos médicos afiliados o contratados.

No hemos podido constatar si el tercero efectivamente accedió, miró o leyó su información personal. Más importante aún, no parece probable que dicha información haya sido enviada ni reenviada y, hasta el día de hoy, no estamos al tanto de que la hayan utilizado indebidamente. Por precaución, queríamos que estuviese al tanto de este incidente y queríamos notificarlo sobre las opciones que tiene a su disposición para protegerse.

¿Qué información estuvo involucrada?
Los correos electrónicos y archivos adjuntos que contenían su información personal a los que es posible que se haya obtenido acceso sin autorización incluían nombres, fechas de nacimiento, números de

Verity Medical Foundation

third party did not have access to your financial account numbers or any of your clinical or medical information.

What We Are Doing About It

Within hours of the incident, the VMF information security team promptly terminated the unauthorized access, disabled the email account, and disconnected the device from the network. The information security team removed all unauthorized emails sent to Foundation or affiliated employees and disabled all email accounts where the user clicked on the link before the email was deleted. There was no unauthorized access to any other Foundation or affiliated employees' accounts.

Since this incident, the Foundation has provided individual counseling and re-education to the individuals involved, is deploying a new mandatory training module for all employees, and has initiated a project to enhance security, including mandating password resets for all employees and disabling unknown URLs.

What You Can Do

To help protect against the risk of identity theft, we are offering you the opportunity to enroll at no cost to you in an identity and credit monitoring service for one year. If you would like to take advantage of this offer, please enroll in the TransUnion – myTrueIdentity Credit Monitoring at www.mytrueidentity.com and enter the unique 12-letter activation code listed [redacted], following the three-step process. Note that this activation code can only be used once. Enclosed is a step-by-step enrollment guide walking you through the process. If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, please call the TransUnion Fraud Response Services toll-free hotline at 855-288-5422 and when prompted, enter the following 6-digit telephone pass code: [redacted]. You will follow the steps to enroll in the offline credit monitoring. You can sign up for the online or offline credit monitoring service anytime between now and May 31, 2019.

As a precautionary measure, we recommend that you monitor your account statements and credit reports carefully. If you detect any unusual or suspicious activity, you should promptly notify the institution or company with which the account is maintained.

You may also want to contact the three U.S. credit reporting agencies to report the incident, to request a report, and to ask that a fraud alert be placed on your credit file.

- Experian.com/help
  888-EXPERIAN (888-397-3742)
  P.O. Box 2104 Allen, TX 75013-0949
- TransUnion.com/credit-help
  888-909-8872
  P.O. Box 1000 Chester, PA 19022

Verity Medical Foundation

identificación de pacientes, números de teléfono, direcciones, nombre de los planes de salud, números de póliza de seguro de salud, números de identificación de suscriptor, identificadores únicos de seguros de salud, historial de solicitudes y reclamos, números de Seguro Social y licencias de conducir. El tercero no tuvo acceso a sus números de cuenta bancaria ni a ninguna información médica o clínica sobre usted.

Lo que estamos haciendo al respecto

Unas horas después del incidente, el equipo de seguridad de la información de VMF puso fin de inmediato al acceso no autorizado, deshabilitó la cuenta de correo electrónico y desconectó el dispositivo de la red. El equipo de seguridad de la información eliminó todos los correos electrónicos no autorizados enviados a la Fundación o a sus empleados afiliados y deshabilitó todas las cuentas de correo electrónico en las que el usuario hizo clic en el enlace antes de la eliminación del correo electrónico. No hubo ningún otro acceso no autorizado a otras cuentas de la Fundación o de sus empleados afiliados.

Desde este incidente, la Fundación ha brindado asesoramiento individual y reeducación a todas las personas involucradas; está implementando un nuevo módulo de capacitación obligatoria para todos los empleados; y ha iniciado un proyecto para mejorar la seguridad, que incluye la orden de reestablecer contraseñas para todos los empleados y deshabilitar las URL desconocidas.

Lo que usted puede hacer

Para ayudar a protegerse del riesgo del robo de identidad, le ofrecemos la oportunidad de inscribirse sin costo alguno a un servicio de monitoreo de identidad y crédito por un año. Si quiere aprovechar esta oferta, inscríbase en myTrueIdentity, el servicio de monitoreo de crédito de TransUnion, en www.mytrueidentity.com, e ingrese el código único de activación de 12 letras indicado [redacted] y siga el proceso de tres pasos. Tenga en cuenta que este código de activación solo puede utilizarse una vez. Se incluye una guía de inscripción paso a paso que lo guiará durante el proceso. Si no cuenta con acceso a internet y desea inscribirse en un servicio de monitoreo de crédito similar pero que no sea electrónico, comuníquese con la línea directa gratuita del Servicio de Respuesta al Fraude de TransUnion llamando al 855-288-5422 y, cuando se le solicite, ingrese el siguiente código de 6 dígitos: [redacted]. Seguirá los pasos para inscribirse en el monitoreo de crédito no electrónico. Podrá registrarse en cualquiera de los servicios de monitoreo de crédito (en línea o no electrónico) en cualquier momento a partir de ahora y hasta el 31 de mayo de 2019.

Como medida de precaución, recomendamos que controle sus estados de cuenta y los informes de crédito con cuidado. Si detecta cualquier actividad inusual o sospechosa, debería dar aviso de inmediato a la institución o la compañía donde está establecida su cuenta.

También recomendamos que se comunique con las tres agencias de informes de crédito de EE. UU. para denunciar el incidente, pedir un informe y solicitar que se coloque una alerta de fraude en su archivo de crédito.

Verity Medical Foundation

- Equifax.com/personal/credit-report-services
  800-349-9960
  P.O. Box 740241 Atlanta, GA 30374-0241

You can also request a free credit report once a year at www.annualcreditreport.com or by calling 877-322-8228.

For More Information

The Foundation has set up a call center to answer questions and provide additional information about this incident. If you have any questions or would like additional information, please call 877-354-7979 from Monday through Friday, 6 a.m. to 6 p.m. (Pacific Time).

We sincerely regret that this incident occurred and apologize for any inconvenience or concern it may cause.

Sincerely,

Kate Gottfried
Chief Compliance, Corporate Responsibility and Privacy Officer

[redacted]

Verity Medical Foundation

- Experian.com/help
  888-EXPERIAN (888-397-3742)
  P.O. Box 2104 Allen, TX 75013-0949
- TransUnion.com/credit-help
  888-909-8872
  P.O. Box 1000 Chester, PA 19022
- Equifax.com/personal/credit-report-services
  800-349-9960
  P.O. Box 740241 Atlanta, GA 30374-0241

También puede solicitar un informe crediticio gratuito una vez al año en www.annualcreditreport.com o llamando al 877-322-8228.

Para obtener más información

La Fundación ha puesto en marcha un centro de llamadas para responder dudas y brindar información adicional sobre este incidente. Si tiene alguna pregunta o si quiere más información, llame al 877-354-7979 de lunes a viernes, de 6 a. m. a 6 p. m. (hora del Pacífico).

Lamentamos profundamente que haya ocurrido este incidente y le pedimos disculpas por cualquier inconveniente o preocupación que pueda ocasionarle.

Atentamente.

Kate Gottfried
Directora de Cumplimiento, Responsabilidad Corporativa y Privacidad
[redacted]