Verity Medical Foundation

400 Race Street, San Jose, CA 95126

February 26, 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 health 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.

<u>What Happened</u>?
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 health information.

We have not been able to conclude whether the third party actually accessed, viewed or read your health 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.

<u>What Information Was Involved</u>?
The emails and attachments containing health information that may have been accessed without authorization included names, dates of birth, patient identification numbers, phone numbers, addresses, name of health plans, treatment received, medical procedures and conditions, laboratory test information, medical equipment information, billing codes, dates of service, information regarding payment for medical care and claims history, health insurance policy numbers, subscriber identification

numbers, unique health insurance identifiers, application and claims history, social security numbers, and driver's licenses. The third party did not have access to your financial account numbers.

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

- 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