

# EXHIBIT A



<<Date>> (Format: Month Day, Year)

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

Dear <<FirstName>> <<LastName>>,

Partnership Health Center (“PHC”) is writing to notify you of an incident that may affect the security of some of your personal information. We take this incident very seriously. This letter provides details of the incident and the resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

**What Happened?** On May 23, 2019, PHC became aware of malware activity in PHC’s computers. PHC is a federally qualified health center engaged in a co-applicant agreement with Missoula County, Montana (“County”). As such, PHC is a department of County. Both PHC and County staff members immediately began an investigation to determine the nature and scope of this event. With the assistance of third-party experts, PHC learned that certain employee emails on impacted computers may have been compromised by malware. The investigation confirmed that the emails may have been subject to unauthorized acquisition between May 22, 2019 and June 5, 2019.

The contents of the at-risk emails were reviewed to identify what personal information was stored within them. On June 26, 2019, after a thorough review of the emails, it was confirmed that some emails contained sensitive information, and identified the individuals potentially impacted by this incident. Once PHC confirmed the individuals who were potentially impacted, PHC worked to obtain contact information for the impacted individuals and then began preparing an accurate written notice of this incident.

**What Information Was Affected?** PHC is providing this notification out of an abundance of caution to anyone whose information was within the at-risk emails. The following types of your information were located in the affected emails: <<ClientDef1(Breach Details Variable Text)>>.

**What Are We Doing?** We take this matter, and the security and privacy of information in our care, very seriously. In addition to conducting a careful investigation, we added additional monitoring tools to watch for suspicious activity, and we enhanced the security of our systems to reduce the risk of future incidents. We are also providing you with notice of this incident, as well as information and resources you may use to better protect your personal information from potential misuse, should you feel it appropriate to do so. We will also be reporting this incident to appropriate regulatory authorities.

**What Can You Do?** Please review the instructions contained in the attached “Steps You Can Take to Protect Your Information.”

**For More Information:** We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-866-775-4209 (toll free), Monday through Friday, 7:00 a.m. to 4:30 p.m., MT.

We sincerely regret any inconvenience this incident may cause you. Partnership Health Center remains committed to safeguarding the information in our care and we will continue to take steps to ensure the security of our systems.

Sincerely,

Laurie Francis  
Executive Director, Partnership Health Center

## Steps You Can Take to Protect Your Information

### **Monitor Your Accounts.**

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

We recommend that you regularly review any Explanation of Benefits statements 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 your statement. If you do not receive regular Explanation of Benefits statements, you can contact your insurer and request that they send such statements following the provision of services in your name or number.

**Credit Reports.** Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

**Security Freeze.** You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, 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. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

#### **Experian**

PO Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

PO Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that 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 seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

#### **Experian**

P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19106  
1-800-680-7289

[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

#### **Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

**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. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state’s Attorney General.