MOSES LAKE
COMMUNITY HEALTH CENTER

HEALTHCARE WITH A HEART

605 South Coolidge Street Moses Lake, WA 98837
MEDICAL |509| 765-0674 DENTAL |509| 766-8977 PHARMACY |509| 764-7426
www.mlchc.org

January 5, 2023

VIA PORTAL

Attorney General Robert Watson Ferguson
Office of the Attorney General
1125 Washington St SE Olympia, WA

Dear Attorney General Ferguson:

I am the Chief Compliance Officer for Moses Lake Community Health Center. I am providing information with respect to a data security incident involving personal information as described below. MLCHC provides primary health services to the underserved and migrant farmworkers in the Grant County area. MLCHC takes the security and privacy of the information that we maintain with utmost seriousness and shall ensure it answers any questions you may have regarding this incident.

Nature of the Security Event

On September 14th, 2023, MLCHC detected a security incident affecting limited parts of our administrative network. Initially it was known that one MLCHC's administrative employee's email account had been the subject of a cyber-attack. The incident was discovered when the third-party threat actor created fraudulent invoices impersonating existing vendors while trying to obtain payment on them using the breached email. They sent fake confirmations to MLCHC's finance department to pay on the received invoices impersonating as the holder of the email account. This same day MLCHC's IT Department began mitigation efforts and review to determine the breadth and depth of this security breach. Steps were taken to secure our network, including but not limited to a system-wide password reset, and MLCHC launched an investigation with the assistance of a third-party forensic firm to determine the nature and scope of the activity. On September 19th, it was discovered that a second email account of another administrative employee had also been the subject of this same cyber-attack. Significantly, the fraudulent transactions did not affect any employees or patients. The investigators determined that between July 26, 2023, and September 19, 2023, an unauthorized person had access to two email accounts within MLCHC's system. Upon learning this, further investigation was completed to determine what information may have been impacted and with whom it was associated.

This extensive investigation and analysis of the data was recently concluded. Upon that determination, MLCHC has worked diligently to identify any impacted individuals to provide notification. On December 13, 2023, MLCHC determined what personal information was affected and to whom it belonged. Although MLCHC has not received evidence of any identity theft or fraud in connection with this incident, MLCHC is notifying those individuals whose information was impacted.

The information that could have been subject to unauthorized access includes the following: name; social security number; date of birth; driver's license number; employee health insurance information; patient identification number; date(s) of service and/or certain clinical information such as treatment/diagnosis information, lab results, or provider name. MLCHC's electronic medical record system was **not** involved or accessed.

Notice to Washington Residents

On January 8th, 2024, MLCHC shall begin providing notice to impacted individuals. Of the 1,189 individuals an extensive number of them were non-patients and the information pertaining to them was also non-clinical. Individuals whose protected health information may have been subject to unauthorized access was less than 500. However, all individuals will receive written notice in substantially the same form as the letter attached herein.

MLCHC is currently finalizing a service provider for complimentary credit monitoring and will send the notification letters with the finalized service provider's information on January 8th, 2023. The finalized letter will be shared with your office at the same time.

Other Steps Taken and To Be Taken

Upon discovering the event, MLCHC moved quickly to investigate and respond to the incident, assess the security of MLCHC's network systems, and identify affected individuals. MLCHC also implemented and will continue to provide additional safeguards and training to its employees. MLCHC is providing access to credit monitoring services for twelve (12) months, through [service provider], to individuals whose personal information was affected by this incident, at no cost to these individuals. Additionally, MLCHC is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. MLCHC is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, the state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. MLCHC has provided written notice of this incident to relevant state regulators, as necessary.

Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at skaur@mlchc.org or (509) 765-0674 ext. 3109.

With Utmost Respect,

Satvir Kaur
Chief Compliance Officer

MOSES LAKE
COMMUNITY HEALTH CENTER

HEALTHCARE WITH A HEART

605 South Coolidge Street Moses Lake, WA 98837
www.mlchc.org
MEDICAL |509| 765-0674 DENTAL |509| 766-8977 PHARMACY |509| 764-7426

[Date]

[Name]

[Street Address]

[City, State, Zip Code]

Dear [Name]:

We are sending this letter to you as part of Moses Lake Community Health Center's commitment to privacy. We take the privacy and security of information that we maintain very seriously and are writing to inform you of a data security incident that involved some of that information. This letter explains what happened, the measures we have taken in response, and offers steps you may consider taking.

What Happened? On September 14th, 2023, MLCHC detected a security incident affecting limited parts of our administrative network. We immediately took steps to secure our network and launched an investigation with the assistance of a third-party forensic firm to determine the nature and scope of the activity. The investigation determined that between July 26, 2023, and September 19, 2023, an unauthorized person had access to two email accounts within our system. Upon learning this, further investigation was completed to determine what information may have been impacted and with whom it was associated. This extensive investigation and analysis of the data was recently concluded. Upon that determination, MLCHC has worked diligently to identify any impacted individuals to provide notification. On December 13, 2023, we determined what personal information was affected and to whom it belonged. We are notifying you now because the investigation recently concluded that information related to you was contained within the files.

What Information Was Involved? Based on our review, some of your information was contained within them, including some or all of the following: name; social security number; date of birth; driver's license number; employee health insurance information; patient identification number; date(s) of service and/or certain clinical information such as treatment/diagnosis information, lab results, or provider name. MLCHC's electronic medical record system was **not** involved or accessed. Again, although it is unlikely that your personal information was viewed, we cannot be fully certain, so we are informing you.

What We Are Doing & What You Can Do. We are constantly updating and improving systems to protect the data we maintain. As a result of this incident, we have implemented additional defensive tools and increased monitoring to help prevent events like these from happening in the future**.** Nonetheless, we ask that you also exercise care to protect yourself from possible abuse of your health information. You can find information on actions you can take to protect yourself on the websites of the Washington State Office of the Attorney General at: http://www.atg.wa.gov/identity-theftprivacy.

If you choose, as a measure of added security, we are offering one year of credit monitoring and reporting services at no cost to you. This service is performed through [service provider] an organization that watches for and reports to your unusual credit activity, such as creating new accounts in your name. [service provider] will also request that the three credit bureaus place a "Fraud Alert" on your credit report. For more information on identity theft prevention, including contact information for the three nationwide credit reporting companies and [service provider], including instructions on how to activate your complimentary membership, please see the additional information provided with this letter.

If you have any questions, please call (509) 765-0674 ext. 3109. We understand that this may pose an inconvenience to you. We sincerely apologize and regret that this situation has occurred. MLCHC is committed to providing quality care, including protecting your personal information.

Sincerely,

Satvir Kaur
Chief Compliance Officer

Additional Steps You Can Take

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre- screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active-duty military personnel have additional rights.