



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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Subject: Notice of Data [Security Incident/Breach])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a recent incident experienced by Yakima Neighborhood Health Services (“YNHS”), located in Yakima, Washington. This incident may have involved some of your personal and protected health information. We are writing to notify you of the incident and inform you about steps you can take to help protect your information.

What Happened: On October 4, 2022, a file containing certain individuals’ personal and protected health information was inadvertently distributed to one individual. Upon learning of this accidental disclosure, YNHS took steps to ensure the recipient deleted the file from their possession.

On November 9, 2022, we determined that your personal and protected health information may have been impacted by this incident. Notably, there is no evidence that your personal information has been misused. However, out of an abundance of caution, we are notifying you about the incident and providing you resources to help you protect your personal information.

What Information Was Involved: The data that was inadvertently disclosed included your name, date of birth, medical record number, and medical treatment location.

What We Are Doing: To help prevent something like this from happening again, we are implementing additional employee training and strengthening our policies and procedures to better protect sensitive data.

What You Can Do: You can follow the recommendations included with this letter to help protect your information.

For More Information: If you have any questions regarding the incident, please call (855) 926-1377, Monday through Friday from 6:00 am to 3:30 pm PST, excluding some major U.S. holidays.

The security of your information is a top priority for YNHS. We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Rhonda Hauff, CEO
Yakima Neighborhood Health Services
12 S. 8th St.
Yakima, WA 98901

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-800-831-5614
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

New York Attorney General

Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.