JacksonLewis

Jackson Lewis P.C.
666 Third Avenue
New York NY 10017-4030
(212) 545-4000 Main
(212) 972-3213 Fax
jacksonlewis.com

DIRECT DIAL: (212) 545-4006
EMAIL ADDRESS: GREGORY.BROWN@JACKSONLEWIS.COM

November 19, 2025

VIA FIRST-CLASS MAIL

Office of the Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104

Re: ***Data Incident Notification***

Dear Sir or Madam:

We are writing to notify your office of a data security incident affecting 3,226 Washington residents. We are submitting this notice as counsel for Anchorage Neighborhood Health Center ("ANHC"), whose mailing address is 4591 Business Park Blvd, Ste. 10, Anchorage, AK 99503.

ANHC was subject to a criminal cyberattack that impacted its systems ("Incident"). With assistance from third-party experts, ANHC took immediate steps to secure its systems and investigate the nature and scope of the Incident. As part of ANHC's extensive investigation, it worked diligently to identify any PII that may have been subject to unauthorized access or acquisition as a result of the Incident.

On or about October 10, 2025, ANHC determined that the Incident may have involved PII related to certain individuals residing in Washington. The categories of PII involved in the Incident are names, dates of birth, social security numbers, driver's license/state ID numbers, medical treatment information, and health insurance information.

Out of an abundance of caution, and in accordance with applicable law, ANHC will provide notice to the affected individuals in the form enclosed as Exhibit A, so that they can take steps to minimize the risk that their information will be misused. ANHC will begin sending these notices shortly. Additionally, ANHC has arranged for the individuals to enroll in free credit monitoring and related services for at least 12 months, including identity theft insurance up to $1,000,000 as well as identity recovery and restoration services.

ANHC treats all sensitive information in a confidential manner and is proactive in the careful handling of such information. Since the Incident, ANHC has taken a number of steps to further secure its systems. Specifically, ANHC has deployed endpoint detection and response within its environment, including 24/7 managed detection and response services, and will continue to utilize this solution on a going forward basis; rebuilt all servers impacted by the Incident; reset all passwords throughout its systems; and is in the process of thoroughly reviewing and upgrading its data security policies and procedures.

ANCHORAGE NEIGHBORHOOD HEALTH CENTER
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

November 19, 2025

<<Incident Notice /Notice of Data Breach>>

Dear <<First Name>> <<Last Name>>,

What Happened

At Anchorage Neighborhood Health Center ("ANHC"), we value and respect the privacy of your information. We are writing to inform you that ANHC was subject to a criminal cyberattack that impacted our systems. With assistance from third-party experts, we took prompt steps to secure our systems and investigate the nature and scope of the Incident. As part of our extensive investigation, we worked diligently to identify any protected health information ("PHI") and personally identifiable information ("PII") that may have been subject to unauthorized access or acquisition as a result of the Incident. On or about October 10, 2025, we determined that the Incident may have impacted PHI or PII related to you. We take this matter very seriously and sincerely apologize for any concern or inconvenience it may cause you.

What Information Was Involved

The Incident may have impacted the following categories of PHI or PII related to you: name, date of birth, Social Security number, driver's license/state identification number, medical treatment information, and/or health insurance information.

What We Are Doing

Out of an abundance of caution, and in accordance with applicable law, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, we have arranged for Experian to provide you <<12/24>> months of free credit monitoring and related services. To enroll, please visit <<URL>> or call <<EXP_TFN>>. Your enrollment code is <<ENROLLMENT>> and the engagement number is <<Engagement Num>>. To receive these services, please be sure to enroll by <<Deadline>>.

We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. As part of our ongoing commitment to cybersecurity, and in response to this Incident, we have implemented additional security enhancements and continue to regularly assess and strengthen our security measures.

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

For More Information

If you have questions or concerns, please call our dedicated call center at 1-844-976-2439, Monday through Friday 6:00 AM – 6:00 PM Pacific Time (excluding major U.S. holidays). We sincerely apologize for any concern or inconvenience this may have caused.

Sincerely,

Anchorage Neighborhood Health Center

ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

Avoiding Medical ID Theft. The following practices can provide additional safeguards to protect against medical identity theft.

- Regularly check the accounts you use regularly to pay for health-related expenses, including bank accounts, health savings accounts, and credit card accounts.
- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

Review Personal Account Statements and Credit Reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-888-298-0045	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Report Suspected Fraud. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a fraud alert, contact the nationwide credit reporting agencies by phone or online. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. If you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Obtain additional information about the steps you can take to avoid identity theft from the following entities:

- ***All U.S. Residents***: The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain

information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the FTC. You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC at 1-877-IDTHEFT (1-877-438-4338) or https://consumer.ftc.gov/features/identity-theft. The mailing address for the FTC is:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580

- ***District of Columbia Residents***: District of Columbia Attorney General, 400 6th Street, NW, Washington, DC 20001; https://oag.dc.gov; 202-727-3400.

- ***Iowa Residents***: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov; 515-281-5164.

- ***New Mexico Residents***: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what information is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting bureaus may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to your employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have additional specific rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf; and by contacting Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

- ***Maryland Residents***: Maryland Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; https://oag.maryland.gov or 1-410-528-8662 or 1-888-743-0023.

- ***New York Residents***: Office of the New York Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov; or 1-800-771-7755.

- ***North Carolina Residents***: North Carolina Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; https://ncdoj.gov; toll-free at 877-566-7226 or 919-716-6000.

- ***Oregon Residents***: Oregon Attorney General's Office, Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us; 877-877-9392.

- ***Rhode Island Residents***: Rhode Island Attorney General, 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in this matter. There are approximately 25 Rhode Island residents potentially impacted by this incident.

JacksonLewis

Jackson Lewis P.C.
666 Third Avenue
New York NY 10017-4030
(212) 545-4000 Main
(212) 972-3213 Fax
jacksonlewis.com

DIRECT DIAL: (212) 545-4006
EMAIL ADDRESS: GREGORY.BROWN@JACKSONLEWIS.COM

November 19, 2025

VIA FIRST-CLASS MAIL

Office of the Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104

Re: ***Data Incident Notification***

Dear Sir or Madam:

We are writing to notify your office of a data security incident affecting 3,226 Washington residents. We are submitting this notice as counsel for Anchorage Neighborhood Health Center ("ANHC"), whose mailing address is 4591 Business Park Blvd, Ste. 10, Anchorage, AK 99503.

ANHC was subject to a criminal cyberattack that impacted its systems ("Incident"). With assistance from third-party experts, ANHC took immediate steps to secure its systems and investigate the nature and scope of the Incident. As part of ANHC's extensive investigation, it worked diligently to identify any PII that may have been subject to unauthorized access or acquisition as a result of the Incident.

On or about October 10, 2025, ANHC determined that the Incident may have involved PII related to certain individuals residing in Washington. The categories of PII involved in the Incident are names, dates of birth, social security numbers, driver's license/state ID numbers, medical treatment information, and health insurance information.

Out of an abundance of caution, and in accordance with applicable law, ANHC will provide notice to the affected individuals in the form enclosed as Exhibit A, so that they can take steps to minimize the risk that their information will be misused. ANHC will begin sending these notices shortly. Additionally, ANHC has arranged for the individuals to enroll in free credit monitoring and related services for at least 12 months, including identity theft insurance up to $1,000,000 as well as identity recovery and restoration services.

ANHC treats all sensitive information in a confidential manner and is proactive in the careful handling of such information. Since the Incident, ANHC has taken a number of steps to further secure its systems. Specifically, ANHC has deployed endpoint detection and response within its environment, including 24/7 managed detection and response services, and will continue to utilize this solution on a going forward basis; rebuilt all servers impacted by the Incident; reset all passwords throughout its systems; and is in the process of thoroughly reviewing and upgrading its data security policies and procedures.

ANCHORAGE NEIGHBORHOOD HEALTH CENTER
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

November 19, 2025

<<Incident Notice /Notice of Data Breach>>

Dear <<First Name>> <<Last Name>>,

What Happened

At Anchorage Neighborhood Health Center ("ANHC"), we value and respect the privacy of your information. We are writing to inform you that ANHC was subject to a criminal cyberattack that impacted our systems. With assistance from third-party experts, we took prompt steps to secure our systems and investigate the nature and scope of the Incident. As part of our extensive investigation, we worked diligently to identify any protected health information ("PHI") and personally identifiable information ("PII") that may have been subject to unauthorized access or acquisition as a result of the Incident. On or about October 10, 2025, we determined that the Incident may have impacted PHI or PII related to you. We take this matter very seriously and sincerely apologize for any concern or inconvenience it may cause you.

What Information Was Involved

The Incident may have impacted the following categories of PHI or PII related to you: name, date of birth, Social Security number, driver's license/state identification number, medical treatment information, and/or health insurance information.

What We Are Doing

Out of an abundance of caution, and in accordance with applicable law, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, we have arranged for Experian to provide you <<12/24>> months of free credit monitoring and related services. To enroll, please visit <<URL>> or call <<EXP_TFN>>. Your enrollment code is <<ENROLLMENT>> and the engagement number is <<Engagement Num>>. To receive these services, please be sure to enroll by <<Deadline>>.

We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. As part of our ongoing commitment to cybersecurity, and in response to this Incident, we have implemented additional security enhancements and continue to regularly assess and strengthen our security measures.

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

For More Information

If you have questions or concerns, please call our dedicated call center at 1-844-976-2439, Monday through Friday 6:00 AM – 6:00 PM Pacific Time (excluding major U.S. holidays). We sincerely apologize for any concern or inconvenience this may have caused.

Sincerely,

Anchorage Neighborhood Health Center

ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

Avoiding Medical ID Theft. The following practices can provide additional safeguards to protect against medical identity theft.

- Regularly check the accounts you use regularly to pay for health-related expenses, including bank accounts, health savings accounts, and credit card accounts.
- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

Review Personal Account Statements and Credit Reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-888-298-0045	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Report Suspected Fraud. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a fraud alert, contact the nationwide credit reporting agencies by phone or online. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. If you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Obtain additional information about the steps you can take to avoid identity theft from the following entities:

- ***All U.S. Residents***: The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain

information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the FTC. You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC at 1-877-IDTHEFT (1-877-438-4338) or https://consumer.ftc.gov/features/identity-theft. The mailing address for the FTC is:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580

- ***District of Columbia Residents***: District of Columbia Attorney General, 400 6th Street, NW, Washington, DC 20001; https://oag.dc.gov; 202-727-3400.

- ***Iowa Residents***: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov; 515-281-5164.

- ***New Mexico Residents***: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what information is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting bureaus may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to your employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have additional specific rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf; and by contacting Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

- ***Maryland Residents***: Maryland Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; https://oag.maryland.gov or 1-410-528-8662 or 1-888-743-0023.

- ***New York Residents***: Office of the New York Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov; or 1-800-771-7755.

- ***North Carolina Residents***: North Carolina Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; https://ncdoj.gov; toll-free at 877-566-7226 or 919-716-6000.

- ***Oregon Residents***: Oregon Attorney General's Office, Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us; 877-877-9392.

- ***Rhode Island Residents***: Rhode Island Attorney General, 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in this matter. There are approximately 25 Rhode Island residents potentially impacted by this incident.