<Return Name>
c/o Cyberscout
<Return Address>
<City> <State> <Zip>

<FirstName> <middle name> <LastName>
<Address1>
<Address2>
<City><State><Zip>

April xx, 2023

Notice of Data Breach

Dear <<First Name>> <<middle name>> <<Last Name>>,

What Happened

We are writing to inform you of a recent incident that may impact the privacy of some of your information. Please be reassured that this is a precautionary letter and there is no evidence at this time that your information has been misused. Below is the description of the situation, and steps you may take should you wish to do so.

On February 13, 2023, Asian Health Services ("AHS") discovered suspicious activity in one of our employee's email accounts. We took steps to secure the email account and launched an investigation with the assistance of third-party experts. We determined that an unauthorized person may have had access to the email account at some time between February 7, 2023, and February 13, 2023. On April 5, 2023, based on the investigation, we confirmed that your information was included in the AHS email account that was accessed by the unauthorized person.

As always, AHS is committed to protecting you and your information, so we are keeping you informed and up to date on how, together, we can continue to ensure your privacy.

What Information Was Involved

The compromised email account may have contained information such as your name, medical record number, date of birth, phone number and/or health information (including diagnoses). We want to let you know that neither your social security number nor financial information were included in the emails. We deeply regret that this has occurred and apologize for any inconvenience or concern caused by this incident.

What We Are Doing

The security experts hired to investigate this incident have assured AHS that the unauthorized person is no longer able to access our email system. We also reported this incident to law enforcement. Furthermore, additional email system safeguards have been implemented. We are continuously exploring ways to further strengthen the security of information in our computer and emails systems. We are also implementing a new layer of protection on all of our systems.

In response to the incident, we are providing impacted adults with access to Single Bureau Credit Monitoring services at no charge. We are also providing parents of impacted minors with access to Cyber Monitoring services, that monitor the dark web, for the parent and minor child. These services provide you with alerts for 12 months from the date of enrollment. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be

provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do

Receiving this letter does not automatically mean you are a victim of identity theft. However, we encourage you to remain vigilant; to continually review your credit report, bank account activity, and bank statements for irregularities or unauthorized items; and to immediately report any unauthorized charges to your financial institution.

If an impacted adult: To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/asianhealthsvcs** and follow the instructions provided. When prompted please provide the following unique code to receive services: <<unique code>>

If an impacted minor: To enroll in Cyber Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/asianhealthsvcs** and follow the instructions provided. When prompted please provide the following unique code to receive services: <<unique code>>. Once you have enrolled yourself, click on your name in the top right of your dashboard and select "Manage Family Protection" then "Add Family Member" to enroll the minor.

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity. There is no evidence that your information has been acquired or misused. However, we encourage you to take full advantage of this service offering. TransUnion representatives can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find general information to further help you protect your personal information on the enclosed Protect Your Information document. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 5:00 a.m. to 6:00 p.m. Pacific time, Monday through Friday, excluding holidays. Please call the help line 1-800-xxx-xxxx and supply the fraud specialist with your unique code listed above. To speak to someone in a language other than English, please let the operator know by telling them the language name in English.

We value your privacy and sincerely regret any inconvenience this matter may cause. Our relationship with you, your confidence in our ability to safeguard your personal information, and your peace of mind are very important to us. Thank you for putting your trust in Asian Health Services. We value your trust and will continue to work to protect your privacy. Please contact us if we can answer questions about this event.

Sincerely,

Joann Wong

Joann Wong, MPH – HIPAA Privacy Officer
Asian Health Services
(Enclosure)

ASIAN HEALTH SERVICES
101 8th Street, Suite 100 | Oakland, CA 94607 | 510-735-3100

Protect Your Information

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. 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 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that 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 can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.
Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II,III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;

5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, ere.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

4. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them, at https://www.identitytheft.gov/.

California Residents: Visit the California Office of Privacy Protection (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 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 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 credit reports to be provided to 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 a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.