



American Indian Health & Services

4141 State Street, A-1, Santa Barbara, CA 93110 • Ph. (805) 681-7356 • FAX (805) 681-7358

May 6, 2019

Name

Address

Dear [Name]:

American Indian Health & Services, Inc. (“AIHS”) is writing to notify you of an incident that may affect the security of some of your personal information. This letter provides details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On March 7, 2019, AIHS discovered a former AIHS employee forwarded certain AIHS emails to her personal email account. While the individual was employed by AIHS at the time the emails were forwarded, because they were forwarded in a manner that conflicts with AIHS policies and procedures, AIHS immediately launched an investigation with the assistance of a third-party computer forensics expert. The investigation included reviewing the email account of this former employee to determine the information contained in the forwarded emails and to whom the information related. The investigation determined the former employee forwarded certain emails between February 26, 2019 and March 6, 2019, some of which contained information relating to certain AIHS employees, patients, and vendors. Although we are unaware of any actual or attempted misuse of your personal information, we are providing you this notification out of an abundance of caution because your information was present in the forwarded emails.

What Information Was Involved? The investigation in this matter confirmed that the following types of personal information may have been accessible as a result of the incident: [data elements].

What Are We Doing. Information privacy and security are among our highest priorities. AIHS has strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to determine the content of the forwarded emails and identify the potentially impacted individuals. We also notified necessary regulatory and law enforcement bodies. In an abundance of caution, we are notifying potentially impacted individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. Although we are unaware of any actual or attempted misuse of information as a result of this incident, we are offering identity theft protection services through ID Experts® to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What Can You Do. You may review the information contained in the attached “Steps You Can Take to Protect Your Information.” You may also enroll to receive the identity theft protection services we are making available to you through ID Experts. AIHS will cover the cost of this service; however, you will need to enroll yourself in this service.

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 [number] (toll free), Monday through Friday 5:00 a.m. to 5:00 p.m., Pacific Time.

We sincerely regret any inconvenience this incident may cause you. AIHS remains committed to safeguarding information in our care.

Sincerely,

[Name]

American Indian Health & Services, Inc.

Steps You Can Take to Protect Your Information

Credit Monitoring and Identity Restoration Services

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling [number] or going to [website] and using the Enrollment Code: XXXX. MyIDCare experts are available Monday through Friday from 5:00 a.m. to 5:00 p.m., Pacific Time. Please note the deadline to enroll is [date].

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, 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 reporting bureaus. To order your free credit report, visit 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.

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	TransUnion P.O. Box 2000 Chester, PA 19016 1-888-909-8872 www.transunion.com/credit-freeze	Equifax PO Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services
---	---	---

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
1. Social Security number;
2. Date of birth;
3. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
4. Proof of current address, such as a current utility bill or telephone bill;
5. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
6. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

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 one 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

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

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

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.