Adventist Health
Simi Valley
C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE
NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY
BREAK
SEQ
CODE 2D
Ver AHS

To Enroll, Please Call:
1-833-719-0090
Or Visit:
https://ide.myidcare.com/adventist-health
Enrollment Code: <<XXXXXXXX>>

January 6, 2020

NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>:

We are writing to tell you about a situation that may have exposed some of your personal information. We take the protection of your information very seriously and are contacting you directly to explain the circumstances of the exposure, the steps we are taking in response to the incident, and the resources that we are making available to you to safeguard your information moving forward.

What Happened
On September 30, 2019 the Adventist Health Information Security Team discovered that a hospital associate was a victim of a phishing attack that compromised their Office 365 account login credentials, including their hospital email account. The perpetrator used the compromised credentials to access the associate's email account in an attempt to redirect invoice payments for the purposes of defrauding the hospital and our vendors.

Upon discovering this incident, our Information Security Team took immediate action to lock down the impacted account. We also began an investigation to understand the scope of the incident, confirmed that other hospital systems were *not* affected, and contacted federal law enforcement.

On October 14, 2019, it was discovered that the compromised email account contained patient information. As of the date of this letter, there has been no indication that any patient information that may have been present in the associate's email account was acquired by hackers. Nevertheless, we are providing this notice out of an abundance of caution because your information was available through the associate's credentials, and potential access to your personal information (before the account was locked down) could not be definitively ruled out.

What Information Was Involved
Information that may have been available through the compromised associate's login credentials include name, date of birth, medical record number, hospital account number, insurance information, and other information related to care received as a patient.

What We Are Doing
Upon discovery of the phishing attack, we quickly disabled and isolated the impacted account and changed the credentials for the impacted associate. An investigation was also conducted to confirm that no other company systems were affected, and that no company or personal data had been emailed out of the compromised account. Additionally, we have engaged federal law enforcement to help find and prosecute the hackers.

We will also continue to provide regular reminders and training for associates on how to spot and avoid being victimized by phishing emails in the future. Cybercriminals will continue to find new ways to target company associates, and we must

all continue to be vigilant against increasingly sophisticated phishing schemes. Additionally, we have taken security measures to strengthen our network against similar incidents.

As an added precaution, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. To enroll please visit https://ide.myidcare.com/adventist-health and use the Enrollment Code provided above.

We are offering this credit monitoring out of an abundance of caution and this offer is not intended and should not be taken to suggest that recipients of the offer are at any substantial risk of harm.

What You Can Do
We want to make sure you are aware of steps that you may take to guard against potential identity theft or fraud. Please review the enclosed "Recommended Steps to Help Protect Your Information" for information regarding your options.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-833-719-0090 or going to https://ide.myidcare.com/adventist-health and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is April 6, 2020.

Again, at this time, there is no evidence that your information has been compromised or misused; however, we encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information
You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the Enrollment Code at the top of this letter when calling or enrolling online, so please do not discard this letter. Please call 1-833-719-0090 or go to https://ide.myidcare.com/adventist-health for assistance or for any additional questions you may have.

Adventist Health Simi Valley sincerely apologizes for the worry and inconvenience that this situation may cause you. Should any new developments arise that may be significant to this data security incident, we will let you know.

Sincerely,

Claudia Kanne, CHC, MBA
Regional Compliance and Privacy Official

MyIDCare™

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Go to https://ide.myidcare.com/adventist-health and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-833-719-0090 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. 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.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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.

5. 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.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.

SEQ
CODE 2D

6. 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.

7. 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.

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

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.