[CAMPBELL COUNTY HEALTH LETTERHEAD]

[DATE]

[ADDRESS]

Dear [NAME],

Campbell County Health recently experienced a potential security incident involving the personal information of some of its current and former employees. We are providing this notice as a precaution to inform potentially affected individuals of the incident and to call your attention to some steps you can take to help protect yourselves. We sincerely regret any concern this may cause you.

What Happened

On January 25, 2017, an unauthorized individual, impersonating a Campbell County Health executive, contacted a Campbell County Health employee requesting W-2 information for Campbell County Health employees. Later that day, before it was determined that the request was fraudulent, the employee provided these files that contained limited information about some of our employees.

What Information Was Involved

The files contained employee information including first and last name, Social Security number and 2016 compensation and deduction information. Employees' home addresses and dates of birth were not provided. Based on our investigation, we have not found any evidence that this incident involves any unauthorized access to or use of any Campbell County Health computer system or network and no protected health information about any employee or patient was provided to any unauthorized individual. Please note, at this time, we are not aware of any fraud or misuse of your information as a result of this incident.

What We Are Doing

Campbell County Health takes the privacy and protection of personal information very seriously, and deeply regrets that this incident occurred. We took steps to address this incident promptly after it was discovered, including working to investigate and remediate the situation. We will also adding to our annual training to employees information about the proper use of sensitive information and how to recognize email scams; provide periodic updates to employees throughout the year as new phishing schemes or email scams come to our attention; and how to potentially recognize a phishing scheme for employees in departments or functions with access to sensitive employee information. In addition, we have contacted law enforcement and will continue to cooperate in their investigation of this incident.

In addition, to help protect your identity, we are offering two years of complimentary identity protection services from a leading identity monitoring services company. These services help detect possible misuse of your personal information and provide you with superior identity protection support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the information in the "Information about Identity Theft Protection" reference guide included here.

What You Can Do

We want to make you aware of steps you can take to guard against fraud or identity theft. We recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. Also, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

As an additional precautionary measure, we also recommend that you file a Form 14039 "Identity Theft Affidavit" with the IRS to help prevent someone from filing a fraudulent tax return in your name. For additional information from the IRS about identity theft, please visit https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft or call 800-908-4490. There may also be similar resources and forms to file for individual states, so we recommend that you contact your state department of revenue directly for more information.

For More Information

For more information about this incident, or if you have additional questions or concerns about this incident, you may contact us directly at [NUMBER] between [TIMES] Mountain time, Monday through Friday or via email at [EMAIL]. Again, we sincerely regret any concern this event may cause you.

Very truly yours,

[NAME]

Information about Identity Theft Protection

To help protect your identity, we are offering a complimentary two-year membership of Experian's® ProtectMyID®. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. Included with this service are fraud resolution services that provide an Experian Fraud Resolution agent to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). While this Fraud Resolution assistance is immediately available to you without any further action on your part, we also encourage you to activate the fraud detection tools available through ProtectMyID® as a complimentary two-year membership. To enroll in these services, visit **http://www.protectmyid.com/redeem** by **February 6, 2019** and use the following activation code: **[ACTIVATION CODE]**. You may also enroll over the phone by calling **877-371-7902** between the hours of 9:00 AM and 9:00 PM (Eastern Time), Monday through Friday and 11:00 AM and 8:00 PM Saturday (excluding holidays). Please provide the following engagement number as proof of eligibility: **PC106206**.

Once you enroll in ProtectMyID, you will have access to the following features:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Fraud Resolution:** Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE**: You receive the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance[1]:** Provides coverage for certain costs and unauthorized electronic fund transfers

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

Review Accounts and Credit Reports: You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For additional information from the IRS about identity theft, please visit https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft or call 800-908-4490. There may be similar resources available at the state level, so we recommend that you contact your state department of revenue directly for more information.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

---

[1] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)
General Contact:

P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:
P.O. Box 740256, Atlanta, GA 30374
Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
General Contact:

P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
General Contact:

P.O. Box 105281
Atlanta, GA 30348
877-322-8228

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872