[CTHP Letterhead/logo]

[date]

[name]
[address 1]
[city], [state] [zip code]

Re: Consolidated Tribal Health Project, Inc. Data Security Event

Dear [First Name] [Last Name],

Consolidated Tribal Health Project, Inc. ("CTHP") is writing to notify you of a data security event that may affect certain information relating to you. While we are unaware of any actual or attempted misuse of this information, this letter contains information about the incident and our response, steps you can take to protect your information, and resources we are making available to help you.

What happened? CTHP has become aware of a data security event involving unauthorized access by a former employee to certain CTHP systems and information maintained by CTHP. CTHP has been working to understand the nature and scope of the incident, and has engaged third-party data forensics experts to assist with its investigation. Law enforcement is also actively investigating this matter, and CTHP is cooperating with this criminal investigation. While the investigations into this incident are ongoing, we determined that the security of some current and former patient, responsible party, and employee information may be affected including your [**PII Data Elements**: name, address, medical information, health insurance information, date of birth, Social Security number, telephone number, financial information and driver's license number].

What we are doing? We take the security of your information very seriously, and apologize for any concern or inconvenience this matter may cause. Our investigation, the investigation of our third-party data forensics experts, and law enforcement's investigation, are all ongoing. Although we are unaware of actual or attempted misuse of your information relating to this incident, to help protect your identity, we have engaged Experian®, the largest credit bureau in the US, to offer you complimentary Fraud Resolution and identity protection for one-year. Instructions on how to enroll and receive these services are included in the attached Notice of Privacy Safeguards.

What you can do. We encourage you to enroll and receive the complimentary credit monitoring and identity restoration services we are offering to you, and to also review the information on how to protect yourself against identity theft and fraud, should you feel it is appropriate to do so, in the enclosed Notice of Privacy Safeguards. We recognize that you may have questions that are not answered in this letter. We have established a confidential, toll free hotline to assist you with questions regarding the incident, this letter or Experian's identity monitoring and protection services. The hotline can be reached at (xxx) xxx-xxxx, Monday through Friday, 6:00 a.m. to 6:00 p.m. P.S.T., and Saturday through Sunday, 8:00 a.m. to 5:00 p.m. P.S.T. You may also visit www.cthp.org for additional information.

We regret any inconvenience this incident may cause. We remain committed to the security of protected information in our care and have taken corrective measures to prevent this situation from recurring.

Sincerely,

[signatory]
Consolidated Tribal Health Project, Inc.

NOTICE OF PRIVACY SAFEGUARDS

We encourage you activate the fraud detection tools available through ProtectMyID® Elite. This product provides you with superior identity protection and resolution of identity theft. To start monitoring your personal information please follows the steps below:

Visit www.protectmyid.com/protect
Provide your activation code: [**code**]

If you have questions or need an alternative to enrolling online, please call xxx-xxx-xxxx and provide Engagement #: [Engagement number]. A credit card is not required for enrollment.

You are also able to immediately contact Experian regarding any fraud issues, and have access to the following features once you initiate ProtectMyID:

- **Experian credit report:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors the Experian file for indicators of fraud.
- **Internet Scan:** Alerts you if your information is found on sites containing compromised data.
- **Address Change Alerts:** Alerts you of changes to your mailing address
- **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*:** Provides coverage for certain costs and unauthorized electronic fund transfers.
- **Lost Wallet Protection:** Get help replacing credit, debit, and medical insurance cards.

Integrate your ProtectMyID membership with the BillGuard app for FREE and receive:

- **Card Fraud Monitoring**: Alerts you when your credit/debit cards are used.
- **Card Concierge**: Resolve billing inquiries and disputes with merchants

If you are a victim of fraud, simply call Experian at xxx-xxx-xxxx by xx/xx/xx and a dedicated Identity Theft Resolution agent will help you restore your identity. Please provide the engagement number in this letter as proof of eligibility.

If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at xxx-xxx-xxxx.

We encourage you to remain vigilant, to review your account statements regularly, 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 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.

At no charge, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below. Information regarding security freezes is also available from these agencies.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You can further educate yourself regarding identity theft, security freezes, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **For California residents**, the Attorney General can be contacted at Attorney General's Office California Department of Justice, Attn: Public Inquiry Unity, P.O. Box 944255, Sacramento, CA 94244-2550; (800) 952-5225, www.privacy.ca.gov. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.ftc.gov/idtheft, 1-877-ID-THEFT (877-438-4338); TTY: 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. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should also be reported to law enforcement.

[CTHP Letterhead/logo]

[Date]

[First Name][Last Name], Next of Kin of [First Name][Last Name]
[Address]
[City],[State][Zip Code]

Re: Consolidated Tribal Health Project, Inc. Data Security Event

To the Next of Kin of [Patient]:

Consolidated Tribal Health Project, Inc. ("CTHP") is writing to notify you of a data security event that may affect certain information relating to your loved one. While we are unaware of any actual or attempted misuse of this information, this letter contains information about the incident and our response, steps you can take to protect your loved one's information, and resources we are making available to help you.

What happened? CTHP has become aware of a data security event involving unauthorized access by a former employee to certain CTHP systems and information maintained by CTHP. CTHP has been working to understand the nature and scope of the incident, and has engaged third-party data forensics experts to assist with its investigation. Law enforcement is also actively investigating this matter, and CTHP is cooperating with this criminal investigation. While the investigations into this incident are ongoing, we determined that the security of some current and former patient, responsible party, and employee information may be affected including your loved one's [**PII Data Elements**: name, address, medical information, health insurance information, date of birth, Social Security number, telephone number, financial information, and driver's license number].

What we are doing? We take the security of your loved one's information very seriously, and apologize for any concern or inconvenience this matter may cause you. Our investigation, the investigation of our third-party data forensics experts, and law enforcement's investigation, are all ongoing. Although we are unaware of actual or attempted misuse of your loved one's information as a result of this incident, we are providing information on steps you may take to help protect your loved one's identity, in the enclosed Notice of Privacy Safeguards, should you feel it is appropriate to do so.

What you can do. We recognize that you may have questions that are not answered in this letter. In addition to reviewing the information in the enclosed Notice of Privacy Safeguards, we have established a confidential, toll-free hotline to assist you with questions regarding the incident and steps you may take to help protect your loved one's identity. The hotline can be reached at (xxx) xxx-xxxx, Monday through Friday, 6:00 a.m. to 6:00 p.m. P.S.T., and Saturday through Sunday 8:00 a.m. to 5:00 p.m. P.S.T. You may also visit www.cthp.org for additional information.

We regret any inconvenience this incident may cause. We remain committed to the security of protected information in our care and have taken corrective measures to prevent this situation from recurring.

Sincerely,

[signatory]
Consolidated Tribal Health Project, Inc.

NOTICE OF PRIVACY SAFEGUARDS

We encourage you to remain vigilant, to review your loved one's account statements regularly, and to monitor your loved one's credit reports for suspicious activity. There are steps you can take to protect your loved one's credit file. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus so long as you verify your authorization to make such a request on behalf of your loved one. To order this 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 this credit report. We recommend contacting the three credit reporting agencies listed below to discuss your particular situation and obtain specific guidance. Once you establish a relationship with the credit reporting agency and verify your authorization to make a request on behalf of your loved one, you can request a copy of your loved one's credit report. A review of the credit report will let you know of any active credit accounts that still need to be closed or any pending collection notices. Be sure to ask for all contact information on accounts currently open in your loved one's name (credit granters, collection agencies, etc.) so that you can follow through with these entities.

You may also request, in writing, that the report list the following alert:

"Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (list yourself, and/or another authorized relative, and/or executor/trustee of the estate—noting the relationship of any individual listed to your family member—and/or a law enforcement agency)."

In most cases, this flag will prevent the opening of new credit accounts in your loved one's name.

Contact for the three major credit bureaus is as follows:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You can further educate yourself regarding identity theft, security freezes, and the steps you can take to protect your loved one's identity, by contacting the Federal Trade Commission or your state Attorney General. **For California residents**, the Attorney General can be contacted at Attorney General's Office California Department of Justice, Attn: Public Inquiry Unity, P.O. Box 944255, Sacramento, CA 94244-2550; (800) 952-5225, www.privacy.ca.gov. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.ftc.gov/idtheft, 1-877-ID-THEFT (877-438-4338); TTY: 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. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should also be reported to law enforcement.

[CTHP Letterhead/logo]

[date], 2015

[name], Parent or Guardian of [minor's name]
[address 1]
[city], [state] [zip code]

Re: Consolidated Tribal Health Project, Inc. Data Security Event

Dear Parent or Guardian of [First Name] [Last Name],

Consolidated Tribal Health Project, Inc. ("CTHP") is writing to notify you of a data security event that may affect some of your child's information. You are being provided this notice on behalf of your child, for whom is identified in our records as a minor potentially affected by this incident. While we are unaware of any actual or attempted misuse of this information, this letter contains information about the incident and our response, steps you can take to protect your child's information, and resources we are making available to help you and your child.

What happen? CTHP has become aware of a data security event involving unauthorized access by a former employee to certain CTHP systems and information maintained by CTHP. CTHP has been working to understand the nature and scope of the incident, and has engaged third-party data forensics experts to assist with its investigation. Law enforcement is also actively investigating this matter, and CTHP is cooperating with this criminal investigation. While the investigations into this incident are ongoing, we determined that the security of certain current and former patient, responsible party and employee information may be affected including your child's [**PII Data Elements**: name, address, medical information, health insurance information, date of birth, Social Security number, telephone number, and driver's license number].

What we are doing. We take the security of protected information very seriously, and apologize for any concern or inconvenience this matter may cause. Our investigation, the investigation of our third-party data forensics experts, and law enforcement's investigation, are all going. Although we are unaware of actual or attempted misuse of your child's information relating to this incident, to help protect your child's information, we are providing you, the parent or guardian, with a complimentary one year membership in Family Secure® from Experian®. Family Secure monitors your Experian credit report to notify you of key changes. In addition, Family Secure will tell you if your loved one has a credit report, a potential sign that his or her identity has been stolen. Instructions on how to enroll and receive these services are included in the attached Notice of Privacy Safeguards.

What you can do. We encourage you to enroll and receive the complimentary credit monitoring and identity restoration services we are offering you and your child, and also review the information on how to protect yourself against identity theft or fraud, should you feel it is appropriate to do so, in the enclose Notice of Privacy Safeguards. We recognize that you may have questions that are not answered in this letter. We have established a confidential, toll free hotline to assist you with questions regarding the incident, this letter or Experian's identity monitoring and protection services. The hotline can be reached at (xxx) xxx-xxxx, Monday through Friday, 6:00 a.m. to 6:00 p.m. P.S.T., and Saturday through Sunday, 8:00 a.m. to 5:00 p.m. P.S.T. You may also visit www.cthp.org for additional information.

We regret any inconvenience this incident may cause. We remain committed to the security of protected information in our care and have taken corrective measures to prevent this situation from recurring.

Sincerely,

[signatory]
Consolidated Tribal Health Project, Inc.

NOTICE OF PRIVACY SAFEGUARDS

To receive the complimentary Family Secure product, you as the parent must enroll at the web site with your activation code listed below. This activation code can only be used by the parent or guardian of the minor. Please keep in mind that once activated, the code cannot be re-used for another enrollment.

Activate Family Secure Now in Three Easy Steps

1. ENSURE **That You Enroll By: [date]** (Your code will not work after this date.)
2. VISIT the **Family Secure Web Site to enroll: http://www.familysecure.com/enroll**
3. PROVIDE **Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call (xxx) xxx-xxxx and provide engagement #: **[engagement number].**

Once your Family Secure membership is activated, you, the parent or legal guardian, of the affected minor will receive the following features:

- Daily monitoring of your Experian credit report with email notification of key changes, as well as monthly "no-hit" reports
- 24/7 credit report access: Unlimited, on-demand Experian reports and scores
- Experian credit score illustrator to show monthly score trending and analysis.

Children, will receive the following features:

- Monthly monitoring to determine whether the enrolled minor in your household has an Experian credit report
- Alerts of key changes to the affected minor's Experian credit report

All Members:

- Identity Theft Resolution assistance: Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies
- $2,000,000 Product Guarantee*

Once your enrollment in Family Secure is complete, we encourage you to remain vigilant, to review your account statements regulator, and to review your credit report for inaccurate or suspicious items. If you have any questions about Family Secure, need help understanding your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at xxx-xxx-xxxx.

We encourage you to remain vigilant, to review your account statements regularly, 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 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.

At no charge, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below. Information regarding security freezes is also available from these agencies.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You can further educate yourself regarding identity theft, security freezes, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **For California residents**, the Attorney General can be contacted at Attorney General's Office California Department of Justice, Attn: Public Inquiry Unity, P.O. Box 944255, Sacramento, CA 94244-2550; (800) 952-5225, www.privacy.ca.gov .The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.ftc.gov/idtheft, 1-877-ID-THEFT (877-438-4338); TTY: 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. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should also be reported to law enforcement.

Consolidated Tribal Health Project, Inc. Notifies Employees and Patients of a Data Security Compromise

[City, state], May xx, 2015 – Consolidated Tribal Health Project, Inc. ("CTHP") has become aware of a data security event involving unauthorized access by a former employee to certain CTHP systems and information maintained by CTHP. CTHP has been working to understand the nature and scope of the incident, and has engaged third-party data forensics experts to assist with its investigation. Law enforcement is also actively investigating this matter, and CTHP is cooperating with this criminal investigation. CTHP is unaware of actual or attempted misuse of information relating to this data security event which may include current and former patient, responsible party, and employee information. Patient and responsible party information that may be affected includes names, addresses, medical information, health insurance information, dates of birth, Social Security numbers and financial information. Employee information that may be affected includes names, Social Security numbers, dates of birth, addresses, health insurance information, medical information, driver's license numbers, financial information and telephone numbers. CTHP will begin mailing notice letters to affected individuals for whom it has current mailing address information written notice of this incident on or about May 11, 2015.

CTHP is encouraging potentially affected individuals to take steps to protect their identity and information, and has established a toll-free call center to answer questions. As the investigations continue, and out of an abundance of caution, CTHP is offering credit monitoring and identity protection services to potentially affected individuals, free of charge, for the next 12 months. Potentially affected individuals can visit www.cthp.org to learn more about this data security event and the support and services being provided. CTHP will also be disclosing this incident to certain state and federal regulators.

CTHP also suggests that potentially affected individuals remain vigilant and seek to protect against possible identity theft or other financial loss by reviewing account statements for any unusual activity, notifying their credit card companies of the potential data compromise, and monitoring their credit reports. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

At no charge, potentially affected individuals can also have these credit bureaus place a "fraud alert" on their files that alerts creditors to take additional steps to verify their identity prior to granting credit in their names. Please note, however, that because it tells creditors to follow certain procedures to protect the individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms an individual's fraud alert, the others are notified to place fraud alerts on that individual's file. Any individual wishing to place a fraud alert, or who has questions regarding their credit report, can contact any one of the following agencies: Equifax, P.O. Box 105069, Atlanta, GA 30348-5069, 800-525-6285, www.equifax.com; Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; or TransUnion, P.O. Box 2000, Chester, PA 19022-2000, 800-680-7289, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at www.ftc.gov/idtheft, or (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should be reported to law enforcement, the Attorney General in the individual's state of residence, and the FTC. State Attorneys General may also have advice on preventing identity theft. Individuals can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or their state's Attorney General. For California residents, the Attorney General can be contacted at Attorney General's Office California Department of Justice, Attn: Public Inquiry Unity, P.O. Box 944255, Sacramento, CA 94244-2550; (800) 952-5225, www.privacy.ca.gov .

To better assist those who may potentially have been affected, CTHP has established a confidential, toll-free hotline to answer questions. This hotline is available Monday through Friday, 6:00 a.m. to 6:00 p.m. P.S.T., and Saturday through Sunday, 8:00 a.m. to 5:00 p.m. P.S.T. and can be reached at (xxx) xxx-xxxx. Potentially affected individuals can also visit www.cthp.org for additional information and updates.

CTHP regrets any inconvenience this data security event may cause its patients, providers, and employees, and is committed to protecting personal information and protected health information in its care. CTHP will continue to thoroughly investigate and respond to this incident and improve its data security. CTHP will continue to cooperate with law enforcement's investigation into this matter.

Media Contact:
Jennifer Coughlin
(215) 977-4081
Jennifer.coughlin@lewisbrisbois.com

###

Consolidated Tribal Health Project, Inc. Notifies Employees and Patients of a Potential Data Security Compromise

[City, state], May xx, 2015 – Consolidated Tribal Health Project, Inc. ("CTHP") has become aware of a data security event involving unauthorized access by a former employee to certain CTHP systems and information maintained by CTHP. CTHP has been working to understand the nature and scope of the incident, and has engaged third-party data forensics experts to assist with its investigation. Law enforcement is also actively investigating this matter, and CTHP is cooperating with this criminal investigation. CTHP is unaware of actual or attempted misuse of information relating to this data security event which may include current and former patient, responsible party, and employee information. Patient and responsible party information that may be affected includes names, addresses, medical information, health insurance information, dates of birth, Social Security numbers, and financial information. Employee information that may be affected includes names, Social Security numbers, dates of birth, addresses, medical information, health insurance information, driver's license numbers, financial information, and telephone numbers. CTHP will begin mailing notice letters to affected individuals for whom it has current mailing address information written notice of this incident on or about May 11, 2015.

CTHP is encouraging potentially affected individuals to take steps to protect their identity and information, and has established a toll-free call center to answer questions. As the investigations continue, and out of an abundance of caution, CTHP is offering credit monitoring and identity protection services to potentially affected individuals, free of charge, for the next 12 months. Potentially affected individuals can visit www.cthp.org to learn more about this data security event and the support and services being provided. CTHP will also be disclosing this incident to certain state and federal regulators.

CTHP also suggests that potentially affected individuals remain vigilant and seek to protect against possible identity theft or other financial loss by reviewing account statements for any unusual activity, notifying their credit card companies of the potential data compromise, and monitoring their credit reports. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

At no charge, potentially affected individuals can also have these credit bureaus place a "fraud alert" on their files that alerts creditors to take additional steps to verify their identity prior to granting credit in their names. Please note, however, that because it tells creditors to follow certain procedures to protect the individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms an individual's fraud alert, the others are notified to place fraud alerts on that individual's file. Any individual wishing to place a fraud alert, or who has questions regarding their credit report, can contact any one of the following agencies: Equifax, P.O. Box 105069, Atlanta, GA 30348-5069, 800-525-6285, www.equifax.com; Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; or TransUnion, P.O. Box 2000, Chester, PA 19022-2000, 800-680-7289, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at www.ftc.gov/idtheft, or (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should be reported to law enforcement, the Attorney General in the individual's state of residence, and the FTC. State Attorneys General may also have advice on preventing identity theft. Individuals can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or their state's Attorney General. For California residents, the Attorney General can be contacted at Attorney General's Office California Department of Justice, Attn: Public Inquiry Unity, P.O. Box 944255, Sacramento, CA 94244-2550; (800) 952-5225, www.privacy.ca.gov .

To better assist those who may potentially have been affected, CTHP has established a confidential, toll-free hotline to answer questions. This hotline is available Monday through Friday, 6:00 a.m. to 6:00 p.m. P.S.T., and Saturday through Sunday, 8:00 a.m. to 5:00 p.m. P.S.T. and can be reached at (xxx) xxx-xxxx. Potentially affected individuals can also visit www.cthp.org for additional information and updates.

CTHP regrets any inconvenience this data security event may cause its patients, providers, and employees, and is committed to protecting personal information and protected health information in its care. CTHP will continue to thoroughly investigate and respond to this incident and improve its data security. CTHP will continue to cooperate with law enforcement's investigation into this matter.

###