LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS AT LAW

888 SW Fifth Avenue, Suite 600
Portland, Oregon 97204-2025
Telephone: 971.712.2800
Fax: 971.712.2801
www.lewisbrisbois.com

SEAN B. HOAR
DIRECT DIAL: 971.712.2795
SEAN.HOAR@LEWISBRISBOIS.COM

December 21, 2016

File No.
f023

VIA ELECTRONIC MAIL

Bob Ferguson
Attorney General
Washington State
1125 Washington Street SE
P.O. Box 40100
Olympia, Washington 98504-0100
E-Mail: securitybreach@atg.wa.gov

Re: Security Breach Notice

Dear Attorney General Ferguson:

I represent Community Health Plan of Washington (CHPW), located in Seattle, Washington. This letter is being sent pursuant to RCW 19.255.010 because CHPW learned on November 30th, 2016, that the personal information of 353,388 residents of Washington may have been involved in a data security incident. The information included names, addresses, dates of birth, Social Security numbers and health care claims.

On November 7th, 2016, CHPW learned of the data security incident that may have affected CHPW member records stored by its technology services provider, Transactions Application Group, Inc., which is owned by NTT Data, Inc. Access to the server which stored these records was immediately disabled. CHPW launched an investigation and a digital forensics firm was engaged to determine what happened and whether any member records were accessed without authorization. CHPW also notified the Washington State Health Care Authority and the Washington State Office of the Insurance Commissioner, and it reported the matter to the Federal Bureau of Investigation ("FBI"). On November 30th, 2016, the investigation confirmed that member records were accessed without authorization.

CHPW has notified all affected patients with the attached letter. It has also provided notice via the attached press release, and through this link on its website: http://chpw.org/about-us/press-room/notice-of-data-security-incident. As referenced in the letter, CHPW will provide 12 months of

credit monitoring and identity protection services to affected patients through Kroll. Please contact me should you have any questions.

Sincerely,

SEAN B. HOAR of
LEWIS BRISBOIS BISGAARD & SMITH LLP

cc. Collin Foulds, General Counsel
Community Health Plan of Washington

COMMUNITY HEALTH PLAN of Washington™

<<MemberFirstName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

<<Date>> (Format: Month Day, Year)

Subject: <<ClientDef1>>(Adult: Data Security Incident / Adult CA: Notice of Data Breach)

Dear <<MemberFirstName>> <<MemberLastName>>,

I am writing to inform you of a data security incident that may have affected your personal information. Community Health Plan of Washington ("CHPW") is committed to providing excellence in your health care and information management. As a community health center-focused, not-for-profit organization, members are our foremost priority. We take the privacy and security of your information very seriously and regret any concern this incident may cause you.

What Happened? On November 7th, 2016, CHPW learned of a data security incident that may have affected CHPW member records stored by our technology services provider. CHPW took immediate measures to disable access to the server which stored these records. We launched an investigation and a digital forensics firm was engaged to determine what happened and if any member records were accessed without authorization. We also notified the Washington State Health Care Authority and Washington State Office of the Insurance Commissioner, and we reported the matter to the Federal Bureau of Investigation ("FBI"). On November 30th, 2016, the investigation confirmed that records were accessed without authorization. The investigation revealed that the initial unauthorized access occurred on January 16th, 2016. This letter serves to inform you of the incident and to share with you all the services we are providing to our members to protect your personal information.

What Information Was Involved? The following types of information appear to have been accessed: names, addresses, dates of birth, Social Security numbers, and certain coding information related to health care claims.

What Are We Doing? We reported the matter to the FBI and are working with them to protect our members' data. In order to further protect you and your information, CHPW is offering you credit and identity monitoring services for 12 months at no cost to you and informing you about additional steps to protect your personal information. We are working with our technology services provider to increase the security of all CHPW member information to prevent similar incidents in the future.

What You Can Do: We encourage you to follow the recommendations on the following page to protect your personal information. You can enroll in the services we are offering through our trusted partner Kroll, a global leader in risk mitigation and response. These free services are available to you immediately upon receiving this notice and can be used at any time during the next 12 months. Visit **http://activatenow.kroll.com** to take advantage of these services. You must activate your identity and credit monitoring services by March 30, 2017.

For More Information: Further information about how to protect your personal information appears on the following page. To receive credit services by mail instead of online or if you have questions or need assistance, please call 1-844-866-3863, 8:00 a.m. to 5:00 p.m. (Pacific Standard Time), Monday through Friday. Specialists in consumer protection are ready for your questions and to provide support.

We are honored to serve you and are committed to protecting your information. Please accept my sincere apology and know we deeply regret any worry or inconvenience this may cause you.

Sincerely,

Leanne Berge
Chief Executive Officer

(see reverse side)

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain aware by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Additional Free Resources: You can obtain information from the consumer reporting agencies, Federal Trade Commission or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

Security Freeze: In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Multi-Language Insert

Multi-language Interpreter Services

ATTENTION: This document includes an important notice. If you cannot read the attached document, we provide language assistance services, free of charge. Please call (1-844) 866-3863 for translation help.

ATENCIÓN: Este documento incluye un aviso importante. Si no puede leer el documento que se encuentra adjunto, le brindaremos servicios de asistencia de idiomas sin cargo. Llame al (1-844) 866-3863 para obtener ayuda en traducciones.

收件人：此文檔包含重要提醒。如果您不能閱讀附錄的文檔，我們提供語言協助服務，此為免費。 請撥打 (1-844) 866-3864, 以取得翻譯協助。

CHÚ Ý: Tài liệu này có chứa một thông báo quan trọng. Nếu Quý vị không thể đọc tài liệu đính kèm, chúng tôi sẽ cung cấp dịch vụ hỗ trợ ngôn ngữ miễn phí. Vui lòng gọi (1-844) 866-3864 để được trợ giúp dịch thuật.

주의: 이 문서는 중요한 공지 내용을 담고 있습니다. 첨부 문서를 읽지 못하시는 경우, 저희는 무료로 언어 지원 서비스를 제공해드립니다. 번역 도움을 받으시려면 (1-844) 866-3864 번으로 연락해 주십시오.

ВНИМАНИЕ! В настоящем документе содержится важное сообщение. Если вы не можете прочитать вложений документ, мы можем бесплатно предоставить переводчика. Если нужна помощь с переводом, звоните по телефону (1-844) 866-3864.

PAUNAWA: Naglalaman ang dokumentong ito ng mahalagang abiso. Kung hindi ninyo mabasa ang nakalakip na dokumento, magbibigay kami ng mga libreng serbisyo ng tulong sa wika. Mangyaring tumawag sa (1-844) 866-3864 para sa tulong sa pagsasaling-wika.

УВАГА! Цей документ містить важливе повідомлення. Якщо ви не можете прочитати вкладений документ, у нас можна безкоштовно скористуватись послугами перекладача. Щоб отримати переклад документа, зателефонуйте за номером (1-844) 866-3864.

ជូនដំណឹង៖ ឯកសារនេះរួមមានទាំងសេចក្តីជូនដំណឹងសំខាន់។
ប្រសិនបើអ្នកមិនអាចអានឯកសារដែលភ្ជាប់បានទេ នោះយើងផ្តល់សេវាជំនួយភាសាដោយឥតគិតថ្លៃ។ សូម
ទូរស័ព្ទទៅលេខ (1-844) 866-3864 សម្រាប់ជំនួយក្នុងការបកប្រែ។

注意:この文書には重要なお知らせが記載されています。添付の文書をお読みになれない場合には、言語アシスタントサービスを無料でご利用いただけます。 翻訳サービスのご依頼は (1-844) 866-3864 までお電話ください。

ማሳሰቢያ፡- ይህ ሰነድ አስፈላጊ መረጃ ይዟል። የተያያዘውን ሰነድ ማንበብ የማይችሉ ከሆነ፣ የቋንቋ እርዳታ በነጻ እንሰጣለን። የትርጉም አገልግሎት የሚፈልጉ ከሆነ፣ እባክዎ በስልክ ቁጥር (1-844) 866-3864 ይደውሉ።

يرجى الانتباه: يحتوي هذه المستند على إخطار هام. إذا كنت غير قادر على قراءة المستند المرفق، فإننا نقدّم خدمات مساعدة لغوية مجانًا. يرجى الاتصال بالرقم (1-844) 866-3864 للحصول على مساعدة بخصوص الترجمة.

ਧਿਆਨ ਦਓਿ: ਇਸ ਦਸਤਾਵੇਜ਼ ਵਿੱਚ ਇੱਕ ਮਹੱਤਵਪੂਰਨ ਸੂਚਨਾ ਸ਼ਾਮਲ ਹੈ। ਜੇਕਰ ਤੁਸੀਂ ਨੱਥੀ ਕੀਤੇ ਹੋਏ ਦਸਤਾਵੇਜ਼ ਨੂੰ ਪੜ੍ਹਨ ਵਿੱਚ ਅਸਮਰੱਥ ਹੋ, ਅਸੀਂ ਮੁਫ਼ਤ ਭਾਸ਼ਾ ਸੇਵਾਵਾਂ ਦਰਾਨ ਕਦਰੇ ਹਾਂ। ਕਿਰਪਾ ਕਰਕੇ ਅਨੁਵਾਦ ਦੀ ਸਹਾਇਤਾ ਲਈ (1-844) 866-3864 ਉੱਤੇ ਕਾਲ ਕਰੋ।

ACHTUNG: Dieses Dokument enthält einen wichtigen Hinweis. Sollten Sie nicht in der Lage sein, das beigefügte Dokument zu lesen, bieten wir Ihnen kostenlose Unterstützung an. Bitte rufen Sie unter der folgenden Nummer an, um Hilfe bei der Übersetzung zu erhalten: (1-844) 866-3864.

ໝາຍເຫດ: ເອກະສານນີ້ລວມມີແຈ້ງການທີ່ສຳຄັນ. ຖ້າທ່ານບໍ່ສາມາດອ່ານເອກະສານທີ່ຕິດຄັດມານີ້ໄດ້, ພວກເຮົາໃຫ້ການຊ່ວຍເຫຼືອດ້ານພາສາໂດຍບໍ່ເສຍຄ່າ. ກະລຸນາໂທຫາ (1-844) 866-3864 ເພື່ອຂໍຄວາມຊ່ວຍເຫຼືອເລື່ອງການແປພາສາ.

Kroll

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Credit Monitoring through TransUnion

You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll investigator, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals buy, sell, and trade personal information. You'll be promptly notified if evidence of your identity information being traded or sold is discovered.

Identity Consultation

You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Restoration

If you become a victim of identity theft, an experienced licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your investigator can dig deep to uncover all aspects of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

1557 NON DISCRIMINATION NOTICE

Community Health Plan of Washington complies with applicable Federal civil rights laws and does not discriminate on the basis of race, color, national origin, age, disability, or sex. Community Health Plan of Washington does not exclude people or treat them differently because of race, color, national origin, age, disability, or sex.

Community Health Plan of Washington:

- Provides free aids and services to people with disabilities to communicate effectively with us, such as:
  - Qualified sign language interpreters
  - Written information in other formats (large print, audio, accessible electronic formats, other formats)
- Provides free language services to people whose primary language is not English, such as:
  - Qualified interpreters
  - Information written in other languages

If you need these services, contact the Appeals and Grievances Department.

If you believe that Community Health Plan of Washington has failed to provide these services or discriminated in another way on the basis of race, color, national origin, age, disability, or sex, you can file a grievance with: Appeals and Grievances Department, by mail at 1111 Third Avenue, Suite 400, Seattle WA 98101, by phone at 1-800-440-1561, by fax at 206-613-8984, or by email at appealsgrievances@chpw.org. You can file a grievance in person or by mail, fax, or email. If you need help filing a grievance, the Appeals and Grievances Department is available to help you. You can also file a civil rights complaint with the U.S. Department of Health and Human Services, Office for Civil Rights electronically through the Office for Civil Rights Complaint Portal, available at https://ocrportal.hhs.gov/ocr/portal/lobby.jsf, or by mail or phone at: U.S. Department of Health and Human Services, 200 Independence Avenue SW., Room 509F, HHH Building, Washington, DC 20201, 1-800-368-1019, 800-537-7697 (TDD).

Complaint forms are available at http://www.hhs.gov/ocr/office/file/index.html.

FOR IMMEDIATE RELEASE

December 21, 2106

FOR INFORMATION CONTACT

Jan Sheeley (206) 613-5046
Jan.Sheeley@chpw.org

MEDIA STATEMENT FROM COMMUNITY HEALTH PLAN OF WASHINGTON (CHPW)

CHPW MEMBERS NOTIFIED OF DATA SECURITY INCIDENT

On November 7th, 2016, Community Health Plan of Washington (CHPW) learned of a data security incident that may have affected CHPW member records stored by its technology services provider. As soon as CHPW learned of the incident, CHPW took immediate measures to disable access to the server which stored these records. CHPW launched an investigation, and a digital forensics firm was engaged to determine what happened and if any member records were accessed without authorization. CHPW notified the Washington State Health Care Authority and the Washington State Office of the Insurance Commissioner of the incident, and reported the matter to the Federal Bureau of Investigation (FBI). On November 30th, 2016, the digital forensics investigation confirmed that member records were accessed without authorization as a result of a vulnerability in CHPW's technology services provider's security. The investigation subsequently revealed that the initial unauthorized access occurred on January 16th, 2016.

CHPW is cooperating with the FBI and actively working to protect member information. It appears that names, addresses, dates of birth, Social Security numbers and certain coding information related to health care claims may have been accessed. Banking and credit information was not contained in the data. On December 21, 2016, CHPW began to notify affected members. All affected members are being offered free credit and identity monitoring services for 12 months and a dedicated hotline and email resources for all questions. CHPW is also working with its technology services provider to increase the security of all CHPW member information and to prevent similar incidents in the future.

"Our highest priority is the protection of our members' confidential information and their trust," said Leanne Berge, CEO of CHPW. "As a community health center-focused, not-for-profit we have the duty to provide transparency in our work and are committed to providing all the resources that our members need to understand this incident and protect themselves."

Background on CHPW:

Founded in 1992 by a network of community and migrant health centers in Washington State, Community Health Plan of Washington is a not-for-profit health plan. The mission of CHPW is to deliver accessible managed care services that meet the needs and improve the health of our communities, and to make managed care participation beneficial for community-responsive providers.

###