WASHINGTON STATE UNIVERSITY

Compliance and Risk Management
Compliance and Civil Rights

July 18th, 2024

To Whom It May Concern:

This is Washington State University's (WSU) response regarding the Change Healthcare data breach. WSU's Cougar Health Services Pharmacy was a client of Change Healthcare. While Change Healthcare has not provided specific information, it provided a substitute notice on or around June 20, 2024, and WSU elected to provide substitute notice to its Pharmacy clients in order to get information out to the clients as soon as possible. Change Healthcare has not provided WSU with names of individuals who may have been impacted. Accordingly, WSU provided substitute notice on July 17, 2024, in accordance with RCW 42.56.590.

1. WSU sent email notice to current and former clients of the WSU Cougar Health Services Pharmacy.

2. WSU has created a website with all of the information that we have received regarding this breach: https://wsu.edu/2024/07/16/third-party-data-breach-impacts-users-of-wsu-pullman-pharmacy/.
   The WSU Cougar Health Services Pharmacy has also posted a notification on their website: https://cougarhealth.wsu.edu/pharmacy/

3. WSU issued a media release on July 17, 2024: https://news.wsu.edu/press-release/2024/07/17/cyberattack-against-third-party-vendor-may-affect-some-wsu-students/

If you have any further questions, please do not hesitate to contact me.

Sally Makamson
WSU System Privacy Officer
Compliance and Civil Rights
Washington State University

July 17, 2024

Subject: Notice of Data Incident

Dear Recipient,

I am writing to inform you of a recent incident experienced by Change Healthcare, which is a third-party service provider of the Washington State University (WSU), Cougar Health Services (CHS) Pharmacy that may have affected the privacy of some of your information. We take this incident seriously, and this letter provides details of the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it appropriate to do so. You are receiving this letter because our records show that you may be a current or former client of the WSU CHS Pharmacy.

What Happened: WSU contracts with Change Healthcare to provide certain electronic pharmacy services involving billing, claims processing and payment. On February 21, 2024, Change Healthcare became aware of a deployment of ransomware in its computer system by a cybercriminal. Change Healthcare retained leading cybersecurity and data analysis experts to assist in the investigation, which began on February 21, 2024**.** On March 7, 2024, Change Healthcare was able to confirm that a substantial quantity of data had been exfiltrated from its environment between February 17, 2024, and February 20, 2024. On March 13, 2024, Change Healthcare obtained a dataset of exfiltrated files that was safe to investigate. On April 22, 2024, following analysis, Change Healthcare publicly confirmed the impacted data could cover a substantial proportion of people in America.

Although Change Healthcare reports its data review is in its late stages and additional customers may be identified as impacted, Change Healthcare has identified certain customers whose members' or patients' data was involved in the incident, but it has not provided names to customers. On June 20, 2024, Change Healthcare began providing notice to its customers. However, WSU has not been notified by Change Healthcare of its list of patients whose data was involved in this incident. On June 20, 2024, Change Healthcare provided on its website a link to its substitute notice more generally so that other customers can provide information to their patients even if they have not been identified as impacted. See https://www.changehealthcare.com/hipaa-substitute-notice.

What Information Was Involved: Change Healthcare cannot confirm exactly what data was affected for each impacted individual, but the data that may have been accessed by unauthorized parties included contact information (such as first and last name, address, date of birth, phone number, and email) and one or more of the following:

- Health insurance information (such as primary, secondary or other health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers).
- Health information (such as medical record numbers, providers, diagnoses, medicines, test results, images, care and treatment).

- Billing, claims and payment information (such as claim numbers, account numbers, billing codes, payment cards, financial and banking information, payments made, and balance due); and/or
- Other personal information such as Social Security numbers, driver's licenses or state ID numbers, or passport numbers.

What We Are Doing: WSU took important steps within its control to minimize the chances of your data being misused as a result of this incident. The connection to Change Healthcare was disabled. WSU CHS Pharmacy has been communicating and monitoring Change Healthcare's communications regarding the steps they were taking in response to this incident including shutting down systems and sever connectivity to prevent further impact. To help prevent something like this from happening again, WSU CHS Pharmacy is implementing additional education and training regarding technical security measures. An internal review is ongoing to identify other recommended corrective actions. Nonetheless, we are providing you with information about steps that you can take to help protect your personal information.

What You Can Do: While Change Healthcare is still investigating whose personal information may have been involved, and WSU CHS Pharmacy is waiting to obtain a list of affected individuals from Change Healthcare, there are steps individuals can take to protect themselves:

- Any individual who believes their information may have been impacted by this incident can enroll in two years of complimentary credit monitoring and identity protection services. Change Healthcare is paying for the cost of these services for two years. To access these services through Change Healthcare please see: https://www.changehealthcare.com/hipaa-substitute-notice.
- Individuals should be on the lookout and regularly monitor the explanation of benefits statements received from their health plan and statements from health care providers, as well as bank and credit card statements, credit reports, and tax returns, to check for any unfamiliar activity.
- If individuals notice any health care services they did not receive listed on an explanation of benefits statement, they should contact their health plan or doctor.
- If individuals notice any suspicious activity on bank or credit card statements or on tax returns, they should immediately contact their financial institution and/or credit card company or relevant agency.
- If an individual believes they are the victim of a crime, they can contact local law enforcement authorities and file a police report.

Individuals may have additional rights available to them depending on the state they live in. You can also read the Change Healthcare notice here: https://www.changehealthcare.com/hipaa-substitute-notice.

For More Information: If you have any questions for WSU CHS Pharmacy regarding this incident please contact Joseph Santos, Quality Assurance & Compliance Coordinator, Cougar Health Services at incident.notification@wsu.edu. The above Change Healthcare link provides contact information for Change Healthcare.

The privacy and security of your information is a top priority for WSU CHS Pharmacy. We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Sunday Henry, MD
Director of Medical Services
Interim Executive Director
Cougar Health Services
Washington State University

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant 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).

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax P.O. Box 105788 Atlanta, GA 30348 1-888-378-4329 www.equifax.com

Experian P.O. Box 9532 Allen, TX 75013 1-800-831-5614 www.experian.com

TransUnion P.O. Box 1000 Chester, PA 19016 1-800-916-8800 www.transunion.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 one year. 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.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. 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. 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov 1-877-438-4338.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

For information on how to request free credit monitoring and ID theft protection please visit https://www.changehealthcare.com/hipaa-substitute-notice.

Enrolling in IDX and Identity Monitoring Services Offered by Change Healthcare: As a safeguard, you may enroll, at no cost to you, in online credit monitoring and identity restoration services provided by IDX for two years. To enroll in these services, please call Change Healthcare at 1-866-262-5342 and ask to enroll.

Individuals must enroll in order for the available services to go into effect, and the monitoring included in the membership must be activated to be effective. Please note that credit monitoring services may not be available for individuals who have not established credit or an address in the

United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score. If you need assistance, IDX will be able to assist you.

We encourage you to take advantage of these protections offered by Change Healthcare and remain vigilant for incidents of potential fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

For specific state information, please see the Change Healthcare notice: https://www.changehealthcare.com/hipaa-substitute-notice.

If you need language assistance, Change Healthcare is offering assistance at the following number:

ATTENTION: If you speak English, language assistance services, free of charge, are available to you. Call 1-866-262-5342 (TTY: 1-866-262-5342).

ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al 1-866-262-5342 (TTY: 1-866-262-5342).

ATANSYON: Si w pale Kreyòl Ayisyen, gen sèvis èd pou lang ki disponib gratis pou ou. Rele 1-866-262-5342 (TTY: 1-866-262-5342)

CHÚ Ý: Nếu bạn nói Tiếng Việt, có các dịch vụ hỗ trợ ngôn ngữ miễn phí dành cho bạn. Gọi số 11-866-262-5342 (TTY: 1-866-262-5342).

ATENÇÃO: Se fala português, encontram-se disponíveis serviços linguísticos, grátis. Ligue para 1-866-262-5342 (TTY: 1-866-262-5342).

注意:如果您使用繁體中文，您可以免費獲得語言援助服務。請致電 1-866-262-5342 (TTY: 1-866-262-5342)。

ATTENTION : Si vous parlez français, des services d'aide linguistique vous sont proposés gratuitement. Appelez le 1-866-262-5342 (ATS : 1-866-262-5342).

PAUNAWA: Kung nagsasalita ka ng Tagalog, maaari kang gumamit ng mga serbisyo ng tulong sa wika nang walang bayad. Tumawag sa 1-866-262-5342 (TTY: 1-866-262-5342).

ВНИМАНИЕ: Если вы говорите на русском языке, то вам доступны бесплатные услуги перевода. Звоните 1-866-262-5342 (телетайп: 1-866-262-5342).

ملحوظة: إذا كنت تتحدث اذكر اللغة، فإن خدمات المساعدة اللغوية تتوافر لك بالمجان. اتصل برقم 1-866-262-5342 (رقم هاتف)

الصم والبكم: 1-866-262-5342) .

ATTENZIONE: In cask la lingua palatal said litigant, so no disponibili servizi di assistenza linguistica gratuiti. Chiamare il numero 1-866-262-5342 (TTY: 1-866-262-5342).

ACHTUNG: Wenn Sie Deutsch sprechen, stehen Ihnen kostenlos sprachliche Hilfsdienstleistungen zur Verfügung. Rufnummer: 1-866-262-5342 (TTY: 1-866-262-5342).

주의: 한국어를 사용하시는 경우, 언어 지원 서비스를 무료로 이용하실 수 있습니다. 1-866-262-5342 (TTY: 1-866-262-5342)번으로 전화해주십시오.

UWAGA: Jeżeli mówisz po polsku, możesz skorzystać z bezpłatnej pomocy językowej. Zadzwoń pod numer 1-866-262-5342 (TTY: 1-866-262-5342).

સુચના: જો તમે ગુજરાતી બોલતા હો, તો નિ:શુલ્ક ભાષા સહાય સેવાઓ તમારા માટે ઉપલબ્ધ છે. ફોન કરો 1-866-262-5342 (TTY: 1-866-262-5342).

เรียน: ถา้ คุณพดู ภาษาไทยคุณสามารถใชบ้ ริการช่วยเหลือทางภาษาไดฟ้ รี โทร 1-866-262-5342 (TTY: 1-866-262-5342).