Notice to Individuals Regarding Privacy Incident

Critical Care, Pulmonary and Sleep Associates, PLLP ("CCPSA"), a private physician practice in Colorado, has recently learned of a breach of part of its secured computer network. CCPSA deeply regrets this incident occurred. We are providing this notice to patients and to individuals who may have been affiliated with CCPSA to let them know about the incident and what we are doing in response.

On November 23, 2018, CCPSA discovered that an unauthorized individual or entity gained access to an employee's CCPSA email account and used the email address to send phishing emails to individuals in the employee's electronic contacts seeking fraudulent financial payments. CCPSA immediately began investigating and took immediate action to block further access and to secure the email account and CCPSA's entire email environment. CCPSA hired a national firm with forensic computer expertise to assist in the investigation and to determine the nature and scope of the breach. CCPSA's forensic investigation concluded on December 14, 2018 and determined that there was unauthorized access to certain CCPSA accounts between August 14 and November 23, 2018. Importantly, CCPSA's electronic medical records platform was NOT compromised or accessed by the hacker.

CCPSA immediately began a detailed analysis and review of all potentially compromised emails and files to identify the names of all individuals who were potentially impacted, as well as the type of information included in these files. Although CCPSA could not fully determine whether, and to what extent, the hacker viewed or copied personal information, regrettably it is possible that personal information was viewed or acquired by the hacker based on the nature of the unauthorized access.

Personal information that may have been accessed could include any of the following: full name, date of birth, address, phone number, email address, clinical information such as dates of service, diagnoses and conditions, labs and diagnostic studies, medications, other treatment information utilized by CCPSA or other providers with whom CCPSA has communicated on behalf of individuals and certain insurance information including member and group numbers, and in some instances costs for services, social security number, and/or driver's license. Credit card and debit card information was NOT involved.

We are committed to safeguarding our patient's personal information and have taken immediate steps to enhance the protections that were already in place before this incident. In addition to our investigation, we reported this breach to law enforcement for further investigation. We made changes to how authorized individuals access our network and required immediate complex password changes to all our employee accounts on November 23. In consultation with IT professionals, we examined and modified certain rules within our computer environment. We are also reinforcing and providing additional mandatory security awareness training to our entire workforce.

We want to make individuals who were potentially affected by this incident aware of steps they may take to promptly guard against any potential harm. We encourage individuals to remain vigilant to the possibility of fraud and identity theft by regularly reviewing their financial statements, credit reports, and explanation of benefits (EOB's) from their health insurers for any unauthorized activity. If individuals identify services that they did not receive or accounts, charges or withdrawals that they did not authorize, they should immediately contact and report to the involved company and to credit reporting agencies. We have reported this incident (but not the identity or personal information concerning potentially impacted individuals) to the three national credit reporting agencies, Experian, Equifax, and TransUnion.

Please review the Information about Identity Theft Protection at the end of this notice. Individuals can obtain information about placing fraud alerts and security freezes from the Federal Trade Commission and the three national credit reporting agencies, as listed below.

Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580
1-877-382-4357 (toll-free) (website) https://www.ftc.gov/

Equifax, P.O. Box 740241, Atlanta, GA 30374-0241;
1-888-548-7878 (toll-free) (website) https://www.equifax.com/personal

Experian, P.O. Box 9532, Allen, TX 75013
1-888-397-3742 (toll-free) (website) http://www.experian.com

TransUnion, P.O. Box 1000, Chester, PA 19022
1-800-916-8800 (toll-free) (website) https://www.transunion.com

CCPSA has arranged for individuals with information involved in this incident to be able to enroll, at no charge to the individuals, in one year of an online credit monitoring service (*my*TrueIdentity) provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. To take advantage of this service, an individual will need to first obtain and use the unique enrollment code found in the notice letter mailed to impacted individuals for whom CCPSA had current mailing addresses. For individuals who did not receive a notice letter but whose information may have been involved, they must contact the toll-free number below to determine if their information was involved and, if so, to receive a free enrollment code. Eligible individuals must enroll no later than **April 30, 2019**. All enrollment codes expire on April 30, 2019.

We sincerely apologize for any inconvenience or concern caused by this incident. CCPSA has partnered with a data breach services company, Epiq, to set up a toll-free call center to help answer questions and provide additional information to individuals whose information may have been involved. If you have been a patient of CCPSA, if you were referred as a patient to CCPSA, or if you were affiliated through employment with CCPSA and you have questions regarding this incident and whether your personal information may have been involved, please call this toll-free number, **1-877-354-7962**, Monday - Saturday, 7 am – 7 pm, Mountain Standard Time (closed on U.S. observed holidays). The call center can provide additional information and answers to questions for those individuals whose personal information was involved in the incident.

Information about Identity Theft Protection

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 below.

Equifax: 1-888-548-7878; P.O. Box 740241, Atlanta, GA 30374-0241;https://www.equifax.com/personal
Experian: 1-888-397-3742; P.O. Box 9532, Allen, TX 75013; http://www.experian.com
TransUnion: 1-800-916-8800; P.O. Box 1000, Chester, PA 19022; https://www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and social security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and 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 identity theft.

Federal Trade Commission, Consumer Response Center: 1-877-382-4357 (toll-free)
600 Pennsylvania Avenue, NW, Washington, DC 20580; https://www.ftc.gov/

For residents of Massachusetts: You also have the right to obtain a police report.

We recommend that you regularly review the explanation of benefits statements that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

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 calling the toll-free fraud number of any of the three national credit reporting agencies listed above or by visiting their websites listed above for more information.