

Buffalo
New York
Chicago
Washington D.C.



www.octillolaw.com

July 30, 2024

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Dear Sir or Madam:

On behalf of Coastal Plains Community MHMR Center (d/b/a Coastal Plains Community Center and Coastal Plains Integrated Health) ("Coastal Plains"), and pursuant to the Personal Information Protection Act ("PIPA"), Md. CodeAnn. Comm. Law 14-3504, this letter provides notice of a recent data security incident. By providing this notice, Coastal Plains does not waive any rights or defenses regarding the applicability of Maryland law, including the applicability of the Maryland data notification laws or personal jurisdiction.

Coastal Plains is a non-profit, government-funded provider of mental health, developmental disabilities, substance use, and primary care services and is an entity covered by the Health Insurance Portability and Accountability Act ("HIPAA") and is providing notification, as well as taking other steps, as required and in compliance with HIPAA.

On November 13, 2023, Coastal Plains discovered suspicious activity on its systems with indicators consistent with a ransomware attack. Coastal Plains immediately began an investigation and took steps to contain the situation, including notifying federal law enforcement and engaging cybersecurity and privacy professionals to assist. The investigation found evidence that unauthorized actors accessed the Coastal Plains systems from November 12, 2023, to November 13, 2023. The investigation determined that unauthorized actors potentially accessed and acquired a limited amount of Coastal Plains data. Coastal Plains provided substitute notice on its website and via media notice on January 9, 2024, in compliance with its internal policies and HIPAA. There is currently no evidence that any information has been misused for identity theft or fraud in connection with the incident.

Coastal Plains identified two (2) Maryland residents may have been affected by this data security incident. While the data elements vary by individual, the elements potentially affected are: name, date of birth, clinical or treatment information, medical provider name, medical record number, health insurance information, and patient account number. Individual written notification is being provided via regular mail today, July 30, 2024. A copy of the mailed letter provided to potentially affected residents is enclosed.

Office of the Attorney General

Page 2

Please feel free to contact me with any questions at (716) 898-2102 or dgreene@octillolaw.com.

Sincerely,

OCTILLO

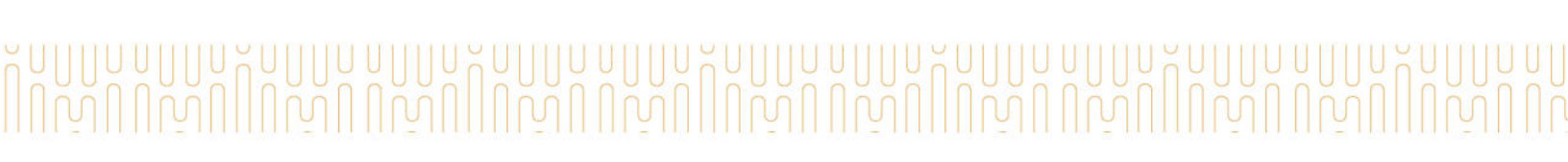
A handwritten signature in black ink, appearing to read 'D. Greene', with a stylized flourish extending to the right.

Daniel P. Greene, Esq.

Certified Information Privacy Professional, United States (CIPP/US)

Certified Information Privacy Professional, Europe (CIPP/E)

Encl.





Coastal Plains

Integrated Health

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

BOARD OF TRUSTEES
Rudy Madrid, Chairman
Pedro Trevino, Jr., Vice-Chairman
Tom Yardley, Secretary
William "Bill" Mills
George Morrill, III
Arnold Cantu
Charles Burns
Eric Ramos
James Liska

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<Date>

<Var Header/Variable 2>

Dear <<Full Name>>,

I am writing to inform you that we, Coastal Plains Community MHMR Center (d/b/a Coastal Plains Community Center and Coastal Plains Integrated Health) ("Coastal Plains" or "we") experienced a data incident in November 2023 ("Incident") which involved your personal information ("Information"). This letter provides you with information about this Incident and where you can direct any questions. Additionally, although we are unaware of any identity theft or fraud in relation to the Incident, as a precaution we have also provided steps you can take to protect your Information.

What Happened?

On November 13, 2023, we discovered suspicious activity on our systems with indicators consistent with a ransomware attack. We immediately began an investigation and took steps to contain the situation, including notifying federal law enforcement and engaging cybersecurity and privacy professionals to assist.

The investigation has found evidence that an unauthorized actor accessed the Coastal Plains systems from November 12, 2023, to November 13, 2023, and after extensive document analysis and review, our investigation determined your Information was potentially accessed and/or acquired. There is currently no evidence that any Information has been misused for identity theft or fraud in connection with the Incident.

What Information Was Involved?

Coastal Plains may have previously received or collected your Information because you or someone known to you provided Information in relation to their employment with us or in order to receive services. Based on the findings of the investigation, the following Information related to you was potentially involved: name, <<Breached Elements>><Variable1>>.

Providing Mental Health and Intellectual Disability Services in Rural South Texas

Leonel B. Trejo, Jr., Chief Executive Officer

What We Are Doing.

Upon becoming aware of the Incident, we immediately implemented measures to further improve the security of our systems and practices, including changing access and authentication controls and enhancing our threat monitoring and detection processes. After determining that an unauthorized actor gained access to our systems, we immediately began analyzing the information involved to confirm the identities of potentially affected individuals and notify them. The Coastal Plains team has worked diligently to complete our investigation, add further technical safeguards to our existing protections, and bring systems back online as quickly and securely as possible. We continue to work with leading privacy and security firms to aid in our response, and we have reported this Incident to relevant government agencies.

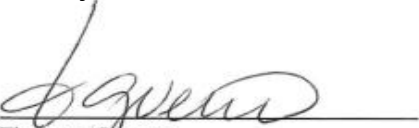
What You Can Do.

Out of an abundance of caution, Coastal Plains encourages individuals to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and to monitor free credit reports for suspicious activity and to detect errors. Under U.S. law, individuals are entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus. Please also review the “Additional Resources” section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

Coastal Plains takes the security of personal information seriously. If you have any questions, you can contact our dedicated toll-free response line at 888-244-3081, Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Standard Time (excluding some U.S. national holidays).

Sincerely,



Theresa Guerra
Director of Authority Functions
Coastal Plains Integrated Health

Encl.

ADDITIONAL RESOURCES

Contact information for the three (3) nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one (1) or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and confirm that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for them as well): (1) full name, with middle initial, and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Protecting Medical Information. If you are concerned about protecting your medical information, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

For Alabama Residents: You may contact the Attorney General's Office for the State of Alabama, Consumer Protection Division, 501 Washington Avenue, Montgomery, AL 36104, <https://www.alabamaag.gov>, 1-800-392-5658.

For California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225. This notification was not delayed as a result of any law enforcement investigation.

For Colorado Residents: You can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

For Illinois Residents: You can obtain information from the credit reporting agencies and the Federal Trade Commission about fraud alerts and security freezes (contact information above). You may contact the Illinois Office of the Attorney General, 100 West Randolph Street, Chicago, IL 60601, https://illinoisattorneygeneral.gov/about/email_ag.jsp, 1-800-964-3013.

For Kansas Residents: You may contact the Kansas Office of the Attorney General, Consumer Protection Division, 120 SW 10th Ave, 2nd Floor, Topeka, KS 66612-1597, <https://ag.ks.gov/>, 1-800-432-2310.

For Kentucky Residents: You may contact the Kentucky Office of the Attorney General, Consumer Protection Division, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, www.ag.ky.gov, 1-800-804-7556.

For Maryland Residents: You may obtain information about steps you can take to avoid identity theft from the Federal Trade Commission (contact information above) and the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

For Minnesota Residents: You may contact the Minnesota Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.ag.state.mn.us, 1-888-743-0023.

For Missouri Residents: You may contact the Missouri Office of the Attorney General, Consumer Protection, 207 W. High St., P.O. Box 899, Jefferson City, MO 65102, www.ago.mo.gov, 1-800-392-8222.

For Nevada Residents: You may contact the Nevada Office of the Attorney General, Bureau of Consumer Protection, 100 N. Carson St, Carson City, NV 89701, www.ag.nv.gov, 1-702-486-3132.

For New Mexico Residents: Consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York Residents: You may obtain information regarding security breach response and identity theft prevention and protection information from the Federal Trade Commission (contact information above) and the New York Office of the Attorney General, Office of the Attorney General, The Capitol, Albany, NY 12224-0341, <https://ag.ny.gov>, 1-800-771-7755.

For North Carolina Residents: You may obtain information about preventing identity theft from the Federal Trade Commission (contact information above) and the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266.

For Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

For Pennsylvania Residents: You may contact the Pennsylvania Office of the Attorney General, Bureau of Consumer Protection, 15th Floor, Strawberry Square, Harrisburg, PA 17120, www.attorneygeneral.gov, 1-800-441-2555.

For Texas Residents: You may contact the Texas Office of the Attorney General, Office of the Attorney General, PO Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov, 1-800-621-0508.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Massachusetts Residents: You have the right to obtain a police report if you are a victim of identity theft.

For North Carolina Residents: You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.