Notice of Data Security Incident

September 11, 2023 – Psych Associates of Maryland LLC d/b/a Bloom Health Centers ("Bloom Health"), experienced a data security incident that may have involved personal and/or protected health information belonging to certain patients and clinicians. Bloom Health has sent notification of this incident by way of U.S. First-Class Mail to potentially impacted individuals with available address information and provided resources to assist them.

Please note that certain affected individuals may have been treated by a Bloom Health doctor at Dominion Hospital. Dominion Hospital is not affiliated with Bloom Health Centers, but allows Bloom Health providers to serve their patients at the hospital. Additionally, certain patients may have been originally seen at companies acquired by Bloom Health, including Psych Associates of Maryland, Comprehensive Behavioral Health, and Kraus Behavioral Health.

On July 5, 2023, Bloom Health became aware of suspicious activity in our email environment. We immediately took steps to secure our environment and launched an investigation with the assistance of a leading computer forensics firm to determine what happened and whether personal or protected health information may have been accessed or acquired during the incident. As a result of the investigation, on July 20, 2023, we identified that certain files within one clinician's mailbox may have been accessed without authorization on or around June 23, 2023, and was then able to obtain access to the associated OneDrive. Out of an abundance of caution, Bloom Health conducted a comprehensive review of all data within the affected account, which was completed on August 7, 2023. Bloom Health then worked diligently to identify up-to-date contact information for all individuals whose information was contained within the mailbox or OneDrive to effectuate formal notification to such individuals, which was finalized on August 28, 2023.

The information varies between individuals, but the affected information may have included name, address, phone number, email address, diagnosis and medication details, health insurance information, and for a limited number of individuals, Social Security number. **Please note that we currently have no evidence to suggest misuse or attempted misuse of this information.**

On September 11, 2023, Bloom Health provided notice of this incident to the potentially impacted individuals whose contact information was identified. In so doing, Bloom Health provided information about the incident and resources that potentially impacted individuals can use to monitor and help protect their personal and/or protected health information. Contact information for some potentially affected individuals was unable to be identified and Bloom Health is providing this website posting as substitute notice to those individuals.

In addition, Bloom Health has established a toll-free call center to answer questions about the incident and to address related concerns. The call center is available Monday through Friday from 9:00 a.m. – 9:00 p.m. Eastern Time, excluding major U.S. holidays, and can be reached at 1-800-939-4170. Bloom Health has also notified the U.S. Health and Human Services Office for Civil Rights of this incident.

The privacy and security of our clinician and patient data is of utmost importance to us, and we deeply regret any concern or inconvenience this incident may cause.

Bloom Health is providing the following information about steps that individuals can take to help protect their information:

What steps can I take to protect my information?

- If you detect suspicious activity on any of your accounts, you should promptly notify the financial institution or company with which the account is maintained. You should also report any fraudulent activity or any suspected incidents of identity theft to law enforcement.
- You may obtain a copy of your credit report at no cost from each of the three nationwide credit reporting agencies. To do so, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. Contact information for the three agencies appears at the bottom of this page.
- Notify your financial institution immediately of any unauthorized transactions made, or new accounts opened, in your name.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.

What should I do to protect myself from payment card/credit card fraud?

We suggest that you review your debit and credit card statements carefully in order to identify any unusual activity. If you see anything that you do not understand or that looks suspicious, you should contact the issuer of the debit or credit card immediately.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. To do so, please visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. Contact information for the three agencies is included in the notification letter and is also listed at the bottom of this page.

How do I put a fraud alert on my account?

You may consider placing a fraud alert on your credit report. This fraud alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact Equifax, Experian or TransUnion and follow the Fraud Victims instructions. To place a fraud alert on your credit accounts, contact your financial institution or credit provider. Contact information for the three nationwide credit reporting agencies is listed below.

Contact information for the three nationwide credit reporting agencies is as follows:

Equifax Security Freeze	Experian Security Freeze	TransUnion (FVAD)
PO Box 105788	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

How do I put a security freeze on my credit reports?

Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

What should I do if my family member's information was involved in the incident and is deceased?

You may choose to notify the three major credit bureaus, Equifax, Experian and TransUnion, and request they flag the deceased credit file. This will prevent the credit file information from being used to open credit. To make this request, mail a copy of your family member's death certificate to each company at the addresses below.

Equifax	**Experian**	**TransUnion**
Equifax Information Services P.O. Box 105169, Atlanta, GA 30348	Experian Information Services P.O. Box 9701 Allen, TX 75013	Trans Union Information Services P.O. Box 2000 Chester, PA 19022

What should I do if my minor child's information is involved in the incident?

You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of a minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft. Contact information for the three national credit reporting agencies may be found above.