CITY OF PHILADELPHIA

Department of Behavioral Health and Intellectual disAbility Services
Promoting Recovery, Resilience & Self Determination

David T. Jones
Commissioner

Jill Bowen, Ph.D.
Deputy Commissioner

Roland Lamb
Deputy Commissioner

Sosunmolu Shoyinka, Ph.D.
Chief Medical Officer

Posted 6/1/20, Updated 6/15/20

The Department of Behavioral Health and Intellectual disAbility Services ("DBHIDS") is posting this notice to alert individuals that their personal health information may have been compromised as a result of a cybersecurity attack. This incident may impact individuals served by:

- the Division of Intellectual disAbility Services ("IDS") which coordinates and administers home and community habilitation, adaptive equipment, behavior and other therapies, early intervention, and residential, respite, employment, and day services for individuals with intellectual disabilities in Philadelphia; and
- Community Behavioral Health ("CBH"), a business associate of DBHIDS which assists DBHIDS in administering the behavioral health Medicaid program (HealthChoices) for the Philadelphia region.

On March 31, 2020, DBHIDS learned that an IDS employee's email account had been compromised as a result of a phishing attack. The Office of Innovation and Technology's Information Security Group ("OIT") immediately secured the account and began an investigation. OIT learned that several additional accounts were compromised: an IDS account discovered April 2, a CBH account discovered on April 15, and a DBHIDS account discovered on April 20. Each account was secured immediately upon discovery. OIT's investigation is ongoing and additional DBHIDS and CBH accounts are being reviewed to determine whether they were also compromised. These attacks are believed to be connected to a series of malicious attacks targeting health care and social services agencies during the COVID-19 global pandemic.

To date, the investigation has been unable to confirm whether unauthorized persons have viewed any emails or attachments in the compromised accounts. The accounts contained demographic and health-related information of individuals receiving services and supports through DBHIDS and CBH, including: names, dates of birth, addresses, account and/or medical record numbers, Social Security numbers, health insurance information, clinical information such as diagnosis, dates of service, provider names, and description of services the individual has applied for or was receiving. For a limited number of individuals served by IDS, the accounts also contained scans of birth certificates, driver's licenses, and Social Security cards.

DBHIDS and CBH are continuing to work with forensics experts to review the emails and attachments in the compromised accounts in order to identify all individuals whose information may have been exposed. DBHIDS and CBH will be sending individual notification letters in the coming weeks and will offer complimentary credit monitoring to all those affected. DBHIDS and CBH encourage everyone to routinely remain vigilant against incidents of identity theft and fraud by regularly reviewing bank account and credit card statements and monitoring health insurance claims or service authorization history for suspicious activity. You are encouraged to take the following steps:

1. Get a copy of your credit report. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. If you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374 1-888-766-0008 www.equifax.com	Experian P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 2000 Chester, PA 19106 1-800-680-7289 www.transunion.com

2. Place a fraud alert or security freeze. If you see suspicious activity, you can ask any of the agencies listed above to place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. You may also ask the agencies to place a "security freeze" on your credit report, which prohibits the credit agency from releasing any information from your credit report without your written authorization. For more information, contact the agencies listed above.

3. Find more information. For more information on actions you can take to protect yourself, you can visit the website of the Pennsylvania Office of Attorney General at: www.attorneygeneral.gov/protect-yourself/identity-theft or the Federal Trade Commission at: www.consumer.ftc.gov.

We sincerely apologize for this incident and the concern it may cause you. The privacy of the people we serve is very important to us and we will continue to do everything we can to protect it. To prevent similar incidents from occurring in the future, we have increased monitoring of network activity and continued to educate users on how to identify and avoid malicious emails. We are in the process of enhancing email security to ensure that similar attacks will not be successful in the future.

If you receive services or support through DBHIDS and have questions or concerns, you can call 1-888-858-1748 for more information. CBH members can call 1-888-545-2600 for more information.