



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, M.D.
Chief Medical Officer

Media Contact: Omoiyé Kinney
(267) 588-6609 Cell #

Cyber Attack Causes HIPAA Breach at the Philadelphia Department of Behavioral Health and Intellectual disAbility Services

Philadelphia-The Department of Behavioral Health and Intellectual disAbility Services (“DBHIDS”) announced today that it is investigating a security breach that may have permitted multiple employee email accounts to be accessed by unauthorized individuals. This incident impacts individuals served by the Division of Intellectual disAbility Services (“IDS”). IDS 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.

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. On April 2, OIT learned that an additional email account within IDS was also compromised. OIT is currently investigating additional DBHIDS employee accounts that may have also been compromised and will update this notice as more information is available.

To date, the investigation has been unable to confirm whether any unauthorized persons have viewed or copied any emails or attachments in the compromised accounts. The accounts contained demographic and health-related information of individuals receiving services and supports through IDS, 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 IDS services the individual has applied for or was receiving. For a limited number of individuals, the accounts also contained scans of birth certificates and Social Security cards.

DBHIDS and OIT 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 will be sending individual notification letters in the coming weeks and will offer complimentary credit monitoring to those affected. DBHIDS encourages 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 explanation of benefits forms for suspicious activity.

“The privacy of the people we serve is among our highest priorities,” said David T. Jones, Commissioner of DBHIDS. “This phishing attack is believed to be part of a series of similar

malicious attacks being carried out against health care and social services agencies stretched thin during the global COVID-19 pandemic. As soon as we learned about this attack, we immediately took action to secure the compromised accounts, prevent future attacks, and inform anyone who may have been impacted. We sincerely regret and apologize for any concern or inconvenience this incident may cause to the people and families we serve.”

To prevent similar incidents from occurring in the future, DBHIDS and OIT have increased monitoring of network activity and continued to educate users on how to identify and avoid malicious emails. The City is in the process of enhancing email security to ensure that similar attacks will not be successful in the future.

Individuals served by DBHIDS with questions or concerns can call 1-888-858-1748 for more information.