Additional 17963

PMHFOS

C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-664-2018
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<Enrollment>>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

May 19, 2021

RE: Notification of Network Event and Potential Data Incident

Dear <<FirstName>> <<LastName>>,

This letter is being sent to notify you of an event involving the computer network of Passavant Memorial Homes Family of Services ("PMHFOS") that may impact your protected health information. PMHFOS includes Passavant Memorial Homes, PDC Pharmacy, Life Enrichment Trust, Life Enrichment Trust of New Jersey, Accessible Dental Services, and Passavant Memorial Homes Foundation.

Description of Network Event

On Saturday, August 15, 2020, through the "Contact Us" webpage of the PMHFOS website (www.pmhfos.org), a communication was sent to PMHFOS by an unauthorized individual. The unauthorized individual obtained the username and password of an authorized PMHFOS user. The unauthorized individual claimed not to have taken malicious actions (such as infecting the system with malware) in light of the "activity" of PMHFOS, presumably referencing PMHFOS' mission and provision of services to individuals with intellectual disabilities, autism, and behavioral health needs.

PMHFOS' Response

Despite the unauthorized individual's claims that no malicious actions were taken, PMHFOS responded immediately. On August 15, 2020, PMHFOS reported the communication to law enforcement authorities and PMHFOS' cyber insurance carrier. PMHFOS immediately engaged forensic investigators to complete a comprehensive review and scan of the PMHFOS network to determine what information, if any, may have been affected. Upon identifying that there were no viruses or malware left behind on the system, and that no data had been encrypted, various system and traffic logs were comprehensively reviewed and assessed.

On September 3, 2020, the forensic investigation confirmed that the unauthorized individual did log into the PMHFOS system for a brief period on Thursday, August 6, 2020, and that protected health information may have been accessible to the unauthorized individual as a result.

PMHFOS engaged forensic experts to complete a "dark web" search for any information related to PMHFOS data for this event, and no information was found.

In addition, once PMHFOS determined the unauthorized individual had access to the PMHFOS system, PMHFOS immediately engaged forensic experts to conduct a thorough and extensive data mining effort to determine what information, if any, may have been accessible to the unauthorized individual. This data mining effort concluded on March 23, 2021. As a result of the data mining effort, PMHFOS determined your information may have

been accessed by the unauthorized individual. This information includes your name, <<data elements>>. We cannot confirm whether this information was actually impacted by this incident; however, out of an abundance of caution, PMHFOS is notifying you of this incident.

In addition to the actions detailed above and notifying the U.S. Department of Health and Human Services, the credit reporting agencies, and certain state regulators of this incident, PMHFOS took numerous steps necessary to prevent future similar occurrences. Of note, the username and password of compromise was disabled, a system-wide password reset (enforcing even stronger passwords) was completed, and all software and hardware specific to network security was updated. In addition, PMHFOS onboarded a new Vice President of Information Technology, and key members of PMHFOS performed additional network and security training to enhance our overall information technology security awareness and acuity. PMHFOS invested in two-factor authentication technology, which requires additional credentials that are only available to the intended user, in addition to the username and password, to be able to access the virtual private network. PMHFOS also invested in additional remote monitoring and patching software and enhanced DNS protection and endpoint protection software. Ultimately, PMHFOS has strengthened – and will continue to strengthen – its computer network and digital capabilities to best enable the provision of optimal supports and services for individuals with intellectual disabilities, autism, and behavioral health needs.

What You Can Do

Although we cannot confirm whether your information was impacted as a result of this incident, again, out of an abundance of caution we are offering guidance and complimentary identity theft protection services. You can review the enclosed **Steps You Can Take To Protect Your Information**, which provides recommendations on what you can do to protect against the possibility of identity theft and fraud, if desired. PMHFOS is also offering complimentary identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

To contact IDX with any questions and/or to enroll in the complimentary IDX services, please call 1-833-664-2018 or visit https://app.idx.us/account-creation/protect, using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9:00AM – 9:00PM Eastern Time. Please note the deadline to enroll is August 19, 2021.

For More Information

We understand you may have questions that are not answered in this letter. To ensure your questions are answered timely, please call our dedicated toll-free line: 1-833-664-2018.

PMHFOS is deeply committed to the provision of optimal supports and services for individuals with intellectual disabilities, autism, and behavioral health needs while maintaining the privacy and security of personal information. We sincerely regret that this incident occurred and apologize for any inconvenience caused. PMHFOS recognizes that you have trusted us with your information, and we humbly apologize. We are grateful for the privilege to serve you in some capacity and look forward to resolving this matter in a timely manner.

Respectfully,

Susan K. Weiss

Susan K. Weiss
Vice President of Human Resources
Passavant Memorial Homes Family of Services

ADDITIONAL STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Monitor Your Accounts: We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity or errors.

Check Credit Reports: Under United States 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. You may also contact the three major credit bureaus directly to request a free copy of your credit report. The contact information for the three major credit bureaus is:

Equifax	Experian	Transunion
P.O. Box 740256	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 10916
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Place a Security Freeze: You may place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. You will need to place a security freeze separately with each of the three major credit bureaus if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, contact the credit reporting agencies.

Place a Fraud Alert: At no charge, you can also have the three major credit bureaus 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. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact the credit reporting agencies.

Additional Resources: If you believe you are the victim of identity theft or have reason to believe that your personal information has been misused, you should contact the Federal Trade Commission and/or your state Attorney General. You can obtain information from these sources about additional steps you can take to protect yourself against identity theft and fraud, as well as information on security freezes and fraud alerts. Instances of known or suspected identity theft should be promptly reported to law enforcement as well as you have the right to file a police report of you ever experience identity theft or fraud. You can contact the Federal Trade Commission at 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; and 1-877-ID-THEFT (1-877-438-4338). For North Carolina residents, the Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, North Carolina 27699; 877-566-7226; and www.ncdoj.gov.