17963

Passavant Memorial Homes Family of Services
C/O ID Experts
100 Passavant Way
Pittsburgh, PA, 15238

<<First Name>> <<Last Name>>
<<Address1>>, <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

<<Date>>

Notification of Network Event and Potential Data Compromise

PMHFOS Stakeholder,

This letter is to inform you of an event that recently occurred pertaining to the computer network of Passavant Memorial Homes Family of Services ("PMHFOS"). PMHFOS includes Passavant Memorial Homes ("PMH"), PDC Pharmacy, Life Enrichment Trust ("LET"), Life Enrichment Trust of New Jersey ("LET NJ"), Accessible Dental Services ("ADS"), and Passavant Memorial Homes Foundation ("PMHF").

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 user. The unauthorized user obtained the username and password of an authorized user, highlighting a potential vulnerability within the computer network. The unauthorized user 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. Nonetheless, as described below, a computer forensics team was immediately engaged. PMHFOS received the initial forensics report on September 3, 2020, which found that the unauthorized user was logged into the PMHFOS system for a brief period on Thursday, August 6, 2020. The report also raised the possibility that the unauthorized user might have seen or removed files containing individually identifiable information.

PMHFOS' Response

PMHFOS responded immediately to this event. On August 15, 2020, PMHFOS reported the communication to law enforcement authorities and PMHFOS' cyber insurance carrier, who immediately engaged forensic investigators to complete a comprehensive review and scan of the PMHFOS network devices and users 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. In addition, PMHFOS engaged the forensic experts to complete a "dark web" search for any information related to PMHFOS data for this event, and no information was found.

However, as of the date of this letter, the forensics team has been unable to rule out the possibility that individually identifiable information may have been accessed or removed from the PMHFOS network. In an abundance of caution, PMHFOS is notifying you of this occurrence and the possibility that your personal information, which in some cases may be protected health information ("PHI") subject to the Health Insurance Portability and Accountability Act ("HIPAA"), may have been compromised. This information may include identifiers such as your full name, social security number, date of birth, home address, diagnosis code, procedure code, disability code, demographic information, financial information (including account numbers), and other information personal to you.

PMHFOS is continuing a thorough forensic investigation into the event. Forensic experts are reviewing all documents and files contained within any folder or file location navigated to by the unauthorized user. This comprehensive datamining effort will more specifically identify the types of information potentially compromised.

In addition to conducting this full forensic investigation, PMHFOS has taken numerous steps necessary to prevent future similar occurrences. Of note, the username and password of compromise has been disabled, a system-wide password reset (enforcing even stronger passwords) has been completed, and all software and hardware specific to network security have been updated. In addition, key members of PMHFOS are currently completing additional network and security training to enhance our overall information technology security awareness and acuity. PMHFOS has also 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 has strengthened – and will continue to strengthen – our 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.

Actions for Persons Who Are Potentially Impacted

Although we cannot confirm whether your information was or was not compromised at this time, out of an abundance of caution we are offering guidance and identity theft protection services in case any of your personal information was impacted by this incident. We encourage maintaining strong password practices for online and electronic accounts, changing these passwords on a regular basis, and not sharing passwords across platforms or with other persons. Additionally, we advise regularly practicing credit monitoring and reviewing your credit history frequently. To further facilitate your ability to do this, PMHFOS is offering complimentary identity theft protection services through ID Experts®, identity monitoring and data protection experts, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identification theft recovery services.

To contact ID Experts with any questions and/or to enroll in the complimentary MyIDCare services, please call 1-833-752-0858 or visit https://app.myidcare.com/account-creation/protect, using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 9:00AM – 9:00PM Eastern Time. Please note the deadline to enroll is January 14, 2021.

Enclosed with this letter is a document describing additional steps you can take to protect your information.

Follow-Up Information

In addition to this communication, all subsequent communications will be available on our website: www.pmhfos.org. If you have any specific questions about this matter, please call our dedicated toll-free line: 1-833-752-0858.

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. Our intention with this notification was to provide any and all potentially impacted persons with the information necessary to protect themselves, and their identity, under the worst-case scenario. PMHFOS recognizes that you have trusted us with your personal 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.