NOTIFICATION OF A DATA BREACH

Memphis, TN — Professional Healthcare Management, Inc. ("PHM")[1] is a business that primarily operates in the home health care services industry and provides related health care services.

PHM announced today that it recently became aware of a data breach impacting its servers, which contained protected health and personal information of some of PHM's clients and employees. PHM is committed to keeping the community informed, communicating about the steps it is taking toward resolution, and ensuring impacted individuals have the tools they need to minimize the impact of the incident. As such, PHM sent notification of this incident to potentially impacted individuals by mail (if possible) and is providing resources to assist them.

On September 14, 2021, PHM discovered that it was the victim of a sophisticated ransomware attack. After discovering the incident, PHM quickly took steps to secure and safely restore its systems and operations. Further, PHM immediately engaged third-party forensic and incident response experts to conduct a thorough investigation of the incident's nature and scope and assist in the remediation efforts. PHM's investigation is ongoing, but after performing a comprehensive review of the impacted data, PHM believes it could contain protected health information.

PHM is notifying those potentially impacted by this incident by mail (if possible) and providing steps that can be taken to protect their information, including complimentary identity monitoring and protection services. PHM recommends that these individuals enroll in the services provided and follow the recommendations contained within the notification letter to increase the likelihood that their information remains protected. ***As of the date of this release, PHM has no evidence indicating misuse of any information. Notification to individuals potentially affected by this incident is being performed out of an abundance of caution and pursuant to the organization's obligations under the Health Insurance Portability and Accountability Act (HIPAA).***

Further, after reviewing the potentially impacted protected health and personal information, PHM determined that it may include first and last name, social security number, health insurance information (Medicaid number, Medicare number and insurance identification number), prescription name(s) and diagnosis code(s). ***Again, as stated above, it is important to note that PHM has no evidence of misuse of any information as of the date of this release.***

In response to this incident, PHM is implementing additional cybersecurity safeguards, enhancing its cybersecurity policies, procedures, and protocols, and implementing additional employee cybersecurity training.

"We take the security and privacy of the information contained in our systems with the utmost seriousness. Further, we were shocked to discover that we were one of the thousands of victims of this type of cyberattack," said Amanda Egner, CIO of PHM. "We are fully committed to protecting the information on our systems and sincerely regret the concern and inconvenience caused by this event. We thank the community, our employees, patients, and partners for their support during this event."

As a precautionary measure, PHM recommends that individuals remain vigilant by closely reviewing their account statements and credit reports. If individuals detect any suspicious activity, PHM strongly advises that they promptly notify the financial institution or company that maintains the account. **Please see "Other Important Information" for more information and tips regarding protecting personal information and safeguarding from identity theft.**

For individuals seeking more information or who have additional questions, please call the dedicated toll-free helpline set up specifically for this purpose at 1-833-760-0502, Monday through Friday, 8:00 a.m. to 8:00 p.m. (EST). In addition, individuals seeking to contact PHM directly may write to Professional Healthcare Management, 7900 Players Forest Drive, Memphis, Tennessee 38119.

[1] Professional Healthcare Management, Inc. is a management company that manages (or previously managed) five healthcare entities (Volunteer Home Care Inc.; Volunteer Home Care of West TN., Inc.; Volunteer Home Care of Middle TN., Inc., which also does business as Quality First Home Care; Springhill Home Health and Hospice; and Affinity Health Care).

OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Credit Report. We recommend that you obtain a free copy of your credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action

Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below to request a copy of your credit report or general identified above inquiries.

Equifax	**Experian**	**TransUnion**
(888) 766-0008	**(888) 397-3742**	**(800) 680-7289**
P.O. Box 740256	P.O. Box 2104	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze (also known as a Credit Freeze). Following is general information about how to request a security freeze from the three credit reporting agencies. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. 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. In addition, in some states, the agency cannot charge you to place, lift or remove a security freeze. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided above).

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion**
P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze	**Security Freeze & Fraud Victim Assistance Dept.** P.O. Box 6790 Fullerton, CA 92834 https://www.transunion.com/credit-freeze

Consider Placing a Fraud Alert on Your Credit Report. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three nationwide credit reporting agencies identified above. Additional information is available at https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Remain Vigilant, Review Your Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you can (1) send a letter to the *Federal Trade*

Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

Take Advantage of Additional Free Resources on Identity Theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). In addition, a copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf 0009_identitytheft_a_recovery_plan.pdf.