The Menninger Clinic Provides Notification of Data Security Incident

HOUSTON, TEXAS: September 24, 2021 – The Menninger Clinic ("Menninger") has learned of a potential data security incident that may have impacted personal information belonging to certain current and former Menninger employees and patients. Menninger has notified potentially impacted individuals of this incident and has provided resources to assist them. This notification provides information about the incident and resources available to assist potentially impacted individuals.

On March 30, 2021, Menninger discovered unusual activity relating to one employee email account. In response, Menninger immediately took steps to investigate the activity and to secure its email environment. Menninger also engaged a leading, independent cybersecurity firm to investigate what happened and whether any personal information may have been impacted. Through the investigation, Menninger learned that certain Menninger employee email accounts were accessed without authorization. Menninger then engaged a cybersecurity firm to review the contents of the impacted email accounts likely to contain personal information. On July 26, 2021, Menninger learned of the individuals whose personal information may have been impacted. Menninger then worked diligently to identify current address information required to notify such individuals of the incident. That process was completed on September 16, 2021.

This incident only potentially impacted information transmitted via email and did not affect any other information systems. Menninger's electronic health records system was not accessed or otherwise impacted by this incident. There is no evidence of the misuse of any information potentially involved in this incident. However, on September 24, 2021, Menninger provided notification of this incident to potentially impacted individuals. In so doing, Menninger provided information about the incident and about steps that potentially impacted individuals can take to help protect their information as well as complimentary credit monitoring and identity protection services.

Menninger takes the security of its employee and patient information very seriously and is taking steps to help prevent a similar event from occurring in the future.

The following personal and protected health information may have been involved in the incident: Social Security numbers, driver's license numbers and other identification numbers, credit card and bank account numbers, dates of birth, medical record numbers, treatment information, billing/claims information, patient account numbers, diagnosis or symptom information, health insurance information, prescription information, electronic signatures, and tax information.

Menninger has established a toll-free call center to answer questions about the incident and to address related concerns. Call center representatives can be reached at 1-833-903-3648.

The privacy and protection of personal information is a top priority for Menninger, and Menninger regrets any inconvenience or concern this incident may cause.

While we have no evidence of the misuse of any potentially impacted individual's information, we are providing the following information to help those wanting to know more about steps they can take to protect themselves and their personal information:

What steps can I take to protect my personal information?

- Please notify your financial institution immediately if you detect any suspicious activity on any of your accounts, including unauthorized transactions or new accounts opened in your name that you do not recognize. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.

- You can request a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To do so, free of charge once every 12 months, please visit http://www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is listed at the bottom of this page.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC's website offers helpful information at http://www.ftc.gov/idtheft.

How do I obtain a copy of my credit report?

You may obtain a free copy of your credit report from each of the three major 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 also can contact one of the following three agencies:

TransUnion	**Experian**	**Equifax**
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
http://www.transunion.com	http://www.experian.com	http://www.equifax.com

How do I put a fraud alert on my account?

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 one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

How do I put a security freeze on my credit reports?

You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or online by following the instructions found at the websites listed below. You will need to provide the following information when requesting a security freeze (note that if you are making a request for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; and (4) address. You may also be asked to provide other personal information such as your email address, a copy of a government-issued identification card, and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. There is no charge to place, lift, or remove a freeze.

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
PO Box 105788	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-909-8872
http://www.equifax.com	http://www.experian.com	http://www.transunion.com

What should I do if my family member's information was involved in the incident and is deceased?

You may choose to notify the three major credit bureaus, Equifax, Experian and TransUnion, and request they flag the deceased credit file. This will prevent the credit file information from being used to open

credit. To make this request, mail a copy of your family member's death certificate to each company at the addresses below.

Equifax	**Experian**	**TransUnion**
Equifax Information Services P.O. Box 105169, Atlanta, GA 30348	Experian Information Services P.O. Box 9701 Allen, TX 75013	Trans Union Information Services P.O. Box 2000 Chester, PA 19022

What should I do if my minor child's information is involved in the incident?

You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of a minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft. Contact information for the three national credit reporting agencies may be found above.