

On May 7, 2018, the Compliance Officer of Hackensack Meridian *Health* Mountainside Medical Center (“Mountainside Medical Center”) notified a number of individuals of an incident possibly involving some of their personal information.

Background Information

On March 9, 2018, we became aware that as a result of a phishing email sent to a Mountainside Medical Center employee, an unauthorized agent had access to the employee’s email account for some time between March 1 and March 9, 2018 without her knowledge. The employee had access to personally identifiable information of Mountainside Medical Center patients as necessary for her job functions.

Immediately upon becoming aware of the unauthorized access, Mountainside Medical Center’s IT support team changed the employee’s credentials and verified that any external access to her account was disabled. The team also conducted an investigation into the issue with the assistance of an outside data security firm and found no attachments were downloaded or viewed, and there is no evidence that any such information was used or further disclosed. While we cannot determine with certainty what information was viewed by the unauthorized agent, it is possible that personal information may have been included and, therefore, accessed as a result of this incident. The accessed emails could have contained the following: first and last name, medical record number, address, telephone number, insurance identification number, insurance type/name, date of the services received, date of birth, telephone number, and in some instances billing codes corresponding to the services received.

Mountainside Medical Center is taking steps to avoid any future similar incidents. In addition to the investigation that has been completed, we are providing re-training to employees regarding vigilance towards suspicious emails. As an additional precaution, to reduce the risk of fraud or identity theft, we are offering affected individuals a one-year membership in Experian’s® IdentityWorksSM at no cost.

We encourage individuals to take precautions to protect the security of their personal information. We recommend that they remain vigilant to prevent identity theft and fraud by monitoring credit reports and financial institution and other account statements. We also advise that they promptly report any suspicious activity or suspected identity theft. In addition, under the federal Fair Credit Reporting Act individuals have the right as a consumer to place fraud alerts on credit reports and to alert potential creditors or lenders of potential fraudulent activity related to the use of their personal information. They may do so by contacting credit reporting agencies, whose contact information is below.

Mountainside Medical Center takes information security and privacy very seriously. Again, we are not able to confirm that personal information was actually accessed by an unauthorized agent, but it could have been. We deeply regret this situation and any inconvenience this may cause.

To Find Out More Information

Mountainside Medical Center has set up a toll-free telephone number where you can learn whether your information may have been affected in this incident, as well as learn more information about the credit monitoring services offered through Experian.

Please call 1-833-486-9260, Monday through Friday, 9:00 a.m. to 5:00 p.m. Eastern Time. (Closed on U.S. observed holidays.)

Contact Information for Credit Reporting Agencies

You can obtain information from these sources on fraud alerts and security freezes.

Equifax

1-800-525-6285
PO Box 105069
Atlanta, GA 30348
www.equifax.com

Experian

1-888-397-3742
PO Box 9701
Allen, TX 75013
www.experian.com

TransUnion

1-800-680-7289 (fraud alert)
1-800-888-4213 (credit
report)
PO Box 2000
Chester, PA 19022
www.transunion.com