NOTICE OF DATA INCIDENT

ABOUT THE DATA PRIVACY EVENT

The Methodist Hospitals, Inc. ("Methodist") recently learned of an incident that may affect the privacy of certain information. Methodist is providing notice of the event so potentially affected individuals may take steps to better protect their personal information, should they feel it appropriate to do so.

FREQUENTLY ASKED QUESTIONS

What Happened? In June 2019, Methodist learned of unusual activity in an employee's email account. We immediately commenced an investigation, working with third-party forensic investigators, to assess the nature and scope of the email account activity. On August 7, 2019, the forensic investigation determined that two (2) Methodist employees fell victim to an email phishing scheme that allowed an unauthorized actor to gain access to their email accounts. The investigation determined that one account was subject to unauthorized access on June 12 and from July 1 to July 8, 2019 and that the other account was subject to unauthorized access from March 13 to June 12, 2019. While we have no evidence of actual or attempted misuse of any information present in the email accounts, we could not rule out the possibility of access to data present in the accounts. In an abundance of caution, we undertook a comprehensive review of the data present in the accounts to confirm what records may be present.

What Information Was Involved? While the information that may have been present in the relevant email accounts varies by individual, it may include: name, address, health insurance subscriber, group, and/or plan number, group identification number, Social Security number, driver's license/state identification number, passport number, financial account number, electronic signature, username and password, date of birth, medical record number, CSN number, HAR number, Medicare/Medicaid number, and medical treatment/diagnosis information.

What Are We Doing? We take this incident and the security of personal information in our care very seriously. Upon learning of this incident, we moved quickly to conduct an investigation, which included working with third-party forensic investigators, to confirm the nature and scope of the event. Additionally, while we have security measures in place to protect data in our systems, we are reviewing our existing policies and procedures and implementing additional safeguards to further protect information. We are also reporting this incident to relevant state and federal regulators.

In response to this invent, Methodist conducted a comprehensive review to identify the individuals whose information was present in the relevant email accounts and is in the process of mailing written notification to those individuals. More information on resources and steps individuals may take to protect their personal information is being provided in the letter mailed to the home address of those individuals whose information may be affected by this incident.

What You Can Do? We encourage individual who may be potentially affected by this incident to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and to monitor credit reports for suspicious activity and to detect errors. You may also review the information contained in the "Steps You Can Take to Protect Your Information" below.

For More Information. For additional information, please contact our dedicated call center at 855-913-0610 Monday through Friday, 8 a.m. to 8 p.m., Central Time (excluding some U.S. national holidays).

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Monitor Accounts

Under U.S. 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.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be

aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); or TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; or www.ncdoj.gov.

For Maryland residents, the Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; or www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island Residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; or 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately two (2) Rhode Island residents whose information may have been present in the relevant emails.