NOTICE OF DATA PRIVACY EVENT

Episcopal Health Services recently discovered an incident that may affect the security of personal information of certain current and former patients. We take this incident very seriously and the confidentiality, privacy, and security of our information is one of our highest priorities.

What Happened? On September 18, 2018 Episcopal Health Services became aware of suspicious activity in employee email accounts. We immediately began an investigation to determine what happened and what information may have been affected. With the assistance of third party forensic investigators, we determined that certain employee email accounts were subject to unauthorized access between August 28, 2018 and October 5, 2018. These email accounts were then reviewed to determine whether they contained any protected health or personal information. On November 1, 2018, Episcopal Health Services determined that the accounts subject to unauthorized access contained protected health information of certain individuals. The types of information contained within the potentially impacted emails are: Social Security number, date of birth, financial account information, medical history information, prescription information, medical record number, treatment or diagnosis information, and health insurance information or policy number. The types of information varied by individual.

Episcopal Health Services is not aware of any reported attempted or actual misuse of any personal information as a result of this event.

What is Episcopal Health Services doing in response to this incident? Episcopal Health Services is committed to, and takes very seriously, its responsibility to protect all data entrusted to us. We are continuously taking steps to enhance data security protections. As part of our incident response, we changed the log-in credentials for all employee email accounts to prevent further unauthorized access. Since then, we have continued ongoing efforts to enhance security controls and to implement additional controls to help protect employee email accounts from unauthorized access. In an abundance of caution, we are also notifying and offering 12 months of complimentary credit monitoring to potentially affected individuals so that they may take further steps to best protect their personal information, should they feel it is appropriate to do so. We are also notifying any required federal and state regulators.

What should I do in response to this incident? Episcopal Health Services encourages you to remain vigilant against incidents of identity theft and fraud. You should review your account statements or your loved ones' account statements for suspicious activity. If you see any unauthorized charges, promptly contact the bank or credit card company. We also recommend reviewing your credit report for inquiries from companies that you have not contacted, accounts you did not open and debts on your accounts that you cannot explain.

What can I do to protect my information?

Monitor Your Accounts.

Credit Reports. Episcopal Health Services encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor their credit reports and explanation of benefits forms for suspicious activity. 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.

Security Freeze 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 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19106 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

Additional Information

Instances of known or suspected identity theft should be reported to law enforcement and the Federal Trade Commission. **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); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them.

Questions regarding the incident should be directed to 1-866-775-4209, Monday through Friday from 9:00a.m. to 6:00 p.m. Eastern Time.