MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Paul T. McGurkin, Jr.
Office: 267-930-4788
Fax: 267-930-4771
Email: pmcgurkin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

April 18, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent Episcopal Health Services located at 327 Beach 19th Street, Far Rockaway, New York 11691, and write to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Episcopal Health Services does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Background

On September 18, 2018 Episcopal Health Services became aware of suspicious activity in employee email accounts. Episcopal Health Services immediately began an investigation to determine what happened and what information may have been affected. With the assistance of third-party forensic investigators, Episcopal Health Services 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. This was a resource heavy review that took several months to complete. On February 26, 2019, Episcopal Health Services determined that the accounts subject to unauthorized access contained protected information of certain individuals. However, the list of potentially affected individuals provided by the vendor did not include addresses for a large number of individuals and included many potential duplicates. Therefore, Episcopal Health Services was required to review its records to attempt to locate the missing addresses and remove

potential duplicates. This process was completed on March 19, 2019. The type of personal information that was included for this New Hampshire resident is their Social Security number.

Notice to New Hampshire Residents

Episcopal Health Services is providing notice of this incident to this one (1) New Hampshire resident whose information is protected by New Hampshire law and five (5) additional New Hampshire residents whose medical information was located in the email account by mailing written notice of this event on April 18, 2019, in substantially the same form as the letter attached hereto as ***Exhibit A***.

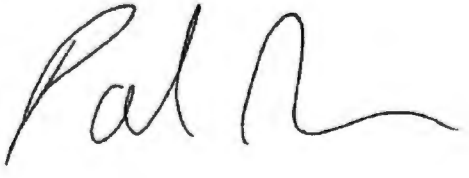
Other Steps Taken and To Be Taken

Episcopal Health Services is committed to, and takes very seriously, its responsibility to protect all data entrusted to it. Episcopal Health Services is continuously taking steps to enhance data security protections. As part of their incident response, Episcopal Health Services changed the log-in credentials for all employee email accounts to prevent further unauthorized access. Since then, Episcopal Health Services has continued ongoing efforts to enhance security controls and to implement additional controls to help protect employee email accounts from unauthorized access. We are also 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4788.

Very truly yours,



Paul T. McGurkin, Jr. of
MULLEN COUGHLIN LLC

PTM/vfr
Enclosure

EXHIBIT A

ST. JOHN'S EPISCOPAL HOSPITAL
EPISCOPAL HEALTH SERVICES INC.

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Event

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Episcopal Health Services is writing to advise you of a recent event that may impact the security of your personal information. While we are unaware of any actual or attempted misuse of the protected health information, we write to provide you with information about the event, steps taken since discovering the event, and what you can do to better protect against potential misuse of your information, should you feel it is appropriate to do so.

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. This was a resource heavy review that took several months to complete. On February 26, 2019, Episcopal Health Services determined that the accounts subject to unauthorized access contained protected health information of certain individuals, including you. However, the list of potentially affected individuals provided by the vendor did not include addresses for a large number of individuals and included many potential duplicates. Therefore, Episcopal Health Services was required to review its records to attempt to locate the missing addresses and remove potential duplicates. This process was completed on March 19, 2019.

What Information Was Involved? The email accounts subject to unauthorized access contained the following types of information relating to you: your <<ClientDef1(name and [data elements])>><<ClientDef2([data elements])>>. Based upon available forensic evidence, Episcopal Health Services was able to confirm that your information was included within email accounts subject to unauthorized access but was unable to confirm whether the email containing your information was actually viewed by the unauthorized actor.

What We Are Doing. 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 potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. We are also notifying any required federal and state regulators.

As an added precaution, we are offering you access to 12 months of free identity monitoring services through Kroll. We encourage you to take advantage of these services. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.
*You have until **July 19, 2019** to activate your identity monitoring services.*
Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-833-231-3362. Additional information describing your services is included with this letter.

What You Can Do. You can review the attached *Steps You Can Take to Protect Against Identity Theft and Fraud.* You can also enroll to receive the free services being offered to you.

For More Information. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated assistance line we've established regarding this incident. Please call 1-833-231-3362 Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time. Please have your membership number ready.

We sincerely regret the inconvenience this incident causes for you. Episcopal Health Services remains committed to safeguarding information in our care and will continue to take proactive steps to enhance data security.

Sincerely,

William Fedorich

William Fedorich
Vice President, General Counsel

Enclosure

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports 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.

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 19106	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

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

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); 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 can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, 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 violator. 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 can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 12 Rhode Island residents impacted by this incident.

Kroll. | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.