Nelson Levine
de Luca & Hamilton LLC
Focused on the Business of Insurance℠

Christopher J. Dilenno
D: 215.358.5161
C: 610.283.5286
cdiienno@nldhlaw.com

518 Township Line Road
Suite 300
Blue Bell, PA 19422
P: 215.358.5100
F: 215.358.5101

February 3, 2014

Attorney General Michael A. Delaney
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: St. Joseph Health System Privacy Event

Dear Sir or Madam:

We represent St. Joseph Health System ("SJHS"), 2801 Franciscan Drive, Bryan, TX 77802, and are writing to notify you of an event that potentially compromised the security of personal information of seventeen (17) New Hampshire residents. By providing this notice, SJHS does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Event

Between Monday, December 16 and Wednesday, December 18, 2013, SJHS experienced a security attack to its computer system by hackers operating from IP addresses in China and elsewhere. SJHS discovered the attack on December 18 and shut down access to the involved computer on that date. SJHS acted quickly, and retained national security and computer forensics experts to thoroughly investigate the scope of the incident. SJHS's investigation, which is ongoing, determined that this attack may have resulted in unauthorized access to certain records related to current and former patients, employees, and employees' beneficiaries.

These records contained a combination of the name, date of birth, social security number, medical information, bank account information, and address for affected individuals. The forensics investigation determined that it is possible that information was accessed, but the investigation has been unable to confirm that any information was actually taken. The involved computer server was shut down when SJHS discovered the security attack on December 18, 2013, so SJHS believes the potential risk to individuals' information ended on that date.

Notice to New Hampshire Residents

Although the investigations are ongoing, at this time it appears that the personal information of seventeen (17) New Hampshire residents could have potentially been accessed as a result of this attack. SJHS is providing the affected individuals, including the New Hampshire residents, with written notice of this incident on or about February 4, 2014, in substantially the same form as the sample notice attached to this letter. Our forensic investigators have not concluded their investigation and if there are additional New Hampshire residents identified we will be providing them with notice and will supplement this notice to you.

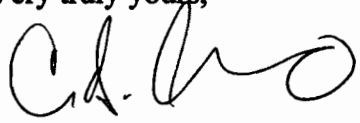
Other Steps Taken and To Be Taken

SJHS takes this matter and the security of personal information in its care very seriously. In addition to providing written and web site notice of this incident to affected individuals, affected individuals are being offered access to one (1) free year of credit monitoring and identity restoration services. SJHS is also providing affected individuals with information on protecting against identity theft and fraud. SJHS is providing written notice of this incident to the U.S. Department of Health and Human Services, additional state and international regulators, and the national consumer reporting agencies. SJHS reported this incident to the United States Federal Bureau of Investigation and continues to work with their ongoing investigation. SJHS is also undergoing additional security measures to strengthen the security of its system.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact Christopher J. DiIenno, Esquire, at 215-358-5161. I kindly request that, if this notice is to be published, all phone numbers and contact information (such as in the letterhead and here) be redacted.

Very truly yours,



Christopher J. DiIenno, Esquire
Nelson Levine de Luca & Hamilton

Enclosures
cc: St. Joseph Health System

EXHIBIT A

St. Joseph
Processing Center • P.O. Box 3825 • Suwanee, GA 30024

February 4, 2014

John Q Sample
123 Main Street
Anytown, US 12345-6789

Dear John Q Sample,*

St. Joseph Health System ("SJHS") based in Bryan, Texas, is writing to inform you of an incident that may affect your personal information.

Between Monday, December 16 and Wednesday, December 18, 2013, SJHS experienced a security attack in which hackers gained unauthorized access to one server on its computer system. SJHS acted quickly, shutting down access to the involved computer on December 18, and hiring national security and computer forensics experts to thoroughly investigate this matter. Our investigation, which is ongoing, determined that this security attack may have resulted in unauthorized access to records for some SJHS patients, employees, and some employees' beneficiaries. These records include your name, and possibly your address.

While it is possible that some information was accessed or taken, the forensics investigation has been unable to confirm this, which is why we are providing this notice to you. The computer was shut down when we discovered the security attack on December 18, 2013, so we believe the potential risk to your information ended on that date. SJHS is working with the United States Federal Bureau of Investigation, which is also looking into this incident.

It is important to note that SJHS has received no reports that any of your personal information has been misused. We take this matter, and the security of your personal information, very seriously. As a precaution, SJHS wants to assist you in protecting your identity even though we are not aware of any misuse of your information and we have been unable to determine whether any data was in fact taken. SJHS has also hired AllClear ID to protect your identity for 12 months at no cost to you. These identity protection services start on the date of this notice and can be used any time over the next 12 months.

- AllClear SECURE: The team at AllClear ID is ready and standing by if you would like help protecting your identity. You are automatically eligible to use this service - there is no action required on your part. If a problem arises, simply call (855) 731-6011 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear maintains an A+ rating at the Better Business Bureau.

*Si Usted prefiere hablar con alguien en Español sobre este asunto, por favor comuniquese con el centro confidencial de suporte al cliente, por llamada gratiz, (855) 731-6011.

- AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to sign-up online at enroll.allclearid.com, or by phone by calling (855) 731-6011 using the following redemption code: **9999999999**. To enroll in this free additional service, you will need to provide your personal information to AllClear ID.

To further protect yourself from identity theft or financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. You can also check your credit by obtaining a free credit report. Under U.S. law, you are entitled to one free credit report every year from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also write, call, or email the three major credit bureaus directly to ask for a free copy of your credit report. Additional information regarding how to contact the credit bureaus and how you may protect your identity is included on the attached document titled "Information About Identity Theft Prevention."

We are sorry for any trouble or concern that this may have caused you. If you have any questions about this incident or this letter, or if you believe you may be a victim of identity theft please contact the call center. The center is confidential, and staffed by professionals trained in identity and credit protection. **You may reach the confidential call center by dialing, toll-free, (855) 731-6011**, Monday through Saturday, 8:00 AM to 8:00 PM U.S. Central Time, excluding major holidays.

Please rest assured that we are taking steps that will prevent this from happening again in the future. We encourage you to take advantage of the free identity and credit protection services described above. SJHS remains committed to the security of your personal information.

Sincerely,

Denise Goffney

Denise Goffney, Corporate Compliance Officer and Privacy Officer
St. Joseph Health System

Information About Identity Theft Prevention

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion, P.O. Box 2000, Chester, PA 19022, 1-800-916-8800, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, you may contact your provider and request them to send such statements following the provision of services in your name or number.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the

appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-800-525-6285, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, www.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion, P.O. Box 2000, Chester, PA 19022, www.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion, P.O. Box 2000, Chester, PA 19022, www.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- Automatic 12 months of coverage
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
You are automatically protected for 12 months from the date the breach incident occurred, as communicated in the breach notification letter you received from Company (the "Coverage Period"). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements
To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, reside in the United States, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8075 to report the fraud prior to expiration of your Coverage Period.
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company.
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft;

Coverage under AllClear Secure Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation")
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur; and
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud;
- You are expected to protect your personal information in a reasonable way at all times. Accordingly, you will not recklessly disclose or publish your Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information, such as, by way of example, in response to "phishing" scams, unsolicited emails, or pop-up messages seeking disclosure of personal information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail	**Mail**	**Phone**
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077