1401 Eye Street NW, Suite 800, Washington, DC 20005 • (202) 783-3300

January 14, 2020

Iliana L. Peters
(202) 626-8327
(202) 403-3902 Direct Fax
ipeters@polsinelli.com

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)
AND FEDERAL EXPRESS

The Honorable Gordon MacDonald
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of a Data Security Incident

Dear Attorney General MacDonald:

We represent Phoenix Children's Hospital ("Phoenix Children's"), in connection with an incident that involved the personal information of one (1) New Hampshire resident, and we provide this notice on behalf of Phoenix Children's pursuant to N.H. REV. STAT. ANN. § 359-C:20. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While Phoenix Children's is notifying you of this incident, Phoenix Children's does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

Phoenix Children's recently determined that an unauthorized individual was able to remotely access the email accounts of seven (7) Phoenix Children's employees. Upon its discovery of the incident, Phoenix Children's immediately took action, including securing the email account credentials and retaining a leading forensic security firm to investigate and confirm the overall security of its email and computer systems.

On November 15, 2019, Phoenix Children's determined that the personal information that was in the impacted email accounts included the name and certain limited medical information of the New Hampshire resident. At this point, Phoenix Children's is not aware of any fraud or identity theft to any individual as a result of this incident and cannot confirm if any personal information was actually obtained by an unauthorized party. Nevertheless, because there was an email account compromise and Phoenix Children's cannot isolate exactly what, if any, information may have been obtained, Phoenix Children's is notifying all individuals whose personal information could have been accessed.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

On January 14, 2020, Phoenix Children's determined that this incident impacted one (1) New Hampshire resident. Phoenix Children's is mailing notification letters to the impacted individual on January 14-15, 2020. Enclosed is a sample of the notice letter that is being sent to the impacted resident via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, Phoenix Children's promptly secured the email accounts to prevent further access. Multi-factor authentication had been enabled prior to this incident. Phoenix Children's also conducted a comprehensive search for any personal information in the impacted email accounts. Finally, Phoenix Children's retained a leading forensic security firm to investigate and confirm the security of its email and computer systems.

CONTACT INFORMATION

Please do not hesitate to contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Iliana L. Peters

Enclosure

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
Parent or Guardian of
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear Parent or Guardian of <<Name 1>>:

NOTICE OF DATA BREACH	
What Happened	The protection and privacy of the personal information with which we are entrusted is one of our highest priorities. Because of this, we are writing to advise you of a recent incident that may have involved some of your minor child's personal information. We recently discovered that Phoenix Children's Hospital was the victim of a cyber attack. Specifically, an unauthorized third party accessed seven of our employees' email accounts between September 5, 2019, and September 20, 2019. We have no reason to believe that your minor child's information has been misused to commit fraud or identity theft; however, we are providing guidance on how you can protect your child's information. Upon learning of the incident, we promptly contained the incident by securing the impacted email accounts to prevent further access. Phoenix Children's also hired a forensic security firm to investigate and confirm security of our email and computer systems.
What Information Was Involved	On November 15, 2019, we determined that the account contained some of your minor child's information. The personal information in the email account included your minor child's name and certain limited health information. **Your minor child's Social Security number was not impacted in this incident.**
What We Are Doing	We take our responsibility to safeguard personal information seriously and apologize for any inconvenience or concern this incident might cause. We are committed to taking steps to help prevent something like this from happening again, including reviewing our technical controls.
What You Can Do	As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").
Other Important Information	You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps to you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting http://www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax	Experian	TransUnion
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at http://www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place 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 the 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. 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 Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

In order to request a security freeze, you may 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.

The credit reporting agencies have three (3) business days after receiving your request to place asecurity freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To remove the security freeze or lift the freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to remove or lift the security freeze for those identified entities or for the specified period of time.

If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the California Attorney General's Office at (916) 445-9555.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, 515-281-5164.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any policereport filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/.

If you cannot read the attached document, please call 1-602-933-1000 for translation help.

Arabic: ملحوظة: إذا كنت تتحدث اذكر اللغة، فإن خدمات المساعدة اللغوية تتوافر لك بالمجان. اتصل برقم 1-602-933-1000) رقم

هـ مصا لمكبلكاو: 1000-933-602-1).

Chinese:注意：如果您使用繁體中文，您可以免費獲得語言援助服務。請致電 1-602-933-1000 TTY: 1-602-933-1000 。

French: Si vous parlez français, des services d'aide linguistique vous sont proposés gratuitement. Appelez le 1-602-933-1000 (ATS : 1-602-933-1000).

Spanish: ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al 1-602-933-1000 (TTY: 1-602-933-1000).

Vietnamese: CHÚ Ý: Nếu bạn nói Tiếng Việt, có các dịch vụ hỗ trợ ngôn ngữ miễn phí dành cho bạn. Gọi số 1-602-933-1000 (TTY: 1-602-933-1000).

This notification was not delayed as a result of a law enforcement investigation.

For More Information	For further information and assistance, please call 866-977-0741 from 7 a.m. to 7 p.m. Mountain Time, send an email message to compliance@phoenixchildrens.com, or send a letter to our postal address, Phoenix Children's Hospital, 1919 E. Thomas Road, Phoenix, AZ 85016, Attention: Chief Compliance/Privacy Officer.

We take our responsibility to safeguard personal information seriously and apologize for any inconvenience or concern this incident might cause.

Sincerely,

Phoenix Children's Hospital
Office of Business Integrity