Children's Hospital Boston

A teaching affiliate of Harvard Medical School

300 Longwood Avenue, Boston, Massachusetts 02115
617-355-6000
www.childrenshospital.org

February 12, 2009

Office of Attorney General Kelly Ayotte
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Dear Security Breach Notification Office:

I am writing to notify you of a possible unauthorized access or use of personal information involving four New Hampshire residents.

On November 12, 2008, one of our employees reported a laptop stolen from a clinical office area. The laptop was not encrypted. Initially, a determination was made that no personal information was saved to the laptop. However, during the course of our review, it was discovered that any information that is viewed on the laptop, such as email, may be accessible in the laptop's "cache" even though the information was not saved. Our Information Security staff used a new tool to search through the email files of the employee who used the laptop to review her email in order to more accurately determine whether there was personal information in her email files that would likely have been stored in the laptop's cache. Our review using this new tool has uncovered several email records that contained a name along with either a social security number, insurance subscriber number, or both. These records affect four New Hampshire residents.

Upon receiving notice of the theft, our Facility Security and Information Security staff undertook an investigation. A police report was filed with the Boston Police Department. We have no indication or evidence that any fraud has been committed or that this personal information has been either retrieved or misused. We intend to offer 2 years of credit monitoring services to individuals whose social security number was involved. In addition, we have worked with the department to ensure that all of its remaining laptops are encrypted, as required under existing Hospital policy, and are issuing reminder notices to other departments about the policy. Finally, we will be providing reinforcement training for the department to reinforce data security policies and ensure that staff understand the risks and requirements around data security, including the importance of adhering to the institution's laptop encryption policy.

We will provide written notice to the affected New Hampshire residents in the next several days. A copy of the letter we will use for this notification is enclosed.

Please contact me if you have any questions or concerns or need further information.

Sincerely,

Mary A. Beckman
Director of Compliance
tel: 857-218-4682

Enclosure

Date

Name
Address
City/Town/State and Zip

Dear :

I am writing to notify you about a possible unauthorized access to or use of your personal information that occurred on or about November 11, 2008, and was identified in late December 2008. The information may have been stored on a laptop computer that was not encrypted and that was stolen from one of our clinical offices. The information included your name **[and your insurance subscriber number but did not include your social security number/,your insurance subscriber number and your social security number].** No address information was included.

We have no indication or evidence that any fraud has been committed or that your personal information has either been retrieved or misused. However, out of an abundance of caution, we wanted to notify you so that you may properly evaluate what actions you may want to consider taking to minimize any potential risks and to protect yourself. We have taken steps to improve information security practices in an effort to prevent this kind of incident from recurring.

You may want to consider placing a security freeze or a fraud alert on your credit report, as described below. A security freeze prohibits a credit reporting agency from releasing any information about 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.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

1-888-397-3742

Trans Union Security Freeze
Found Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
1-800-680-7289

Contact each company to be sure you understand the information you must provide and the fee, if any, that will apply.

In addition, you may place a "fraud alert" on your credit file by contacting the fraud department of any one of the three major credit bureaus. The fraud alert requires that creditors contact you before opening any new accounts or making any changes to your existing accounts. When you place a fraud alert on your credit file, all three credit bureaus are required by law to automatically send a credit report free of charge to you. This "one-call" fraud alert will remain in your credit file for at least 90 days. When you receive your credit reports, review them carefully for any unexplained activity.

We recommend that your review your credit card and other financial account information regularly for any suspicious or unauthorized activity. *[To help you detect possible misuse of your personal information, we are providing you with a complimentary 2-year membership in Experian's Triple Alert credit monitoring service at no cost to you. This will allow for your credit reports to be monitored at the three national credit reporting companies (Experian, Equifax and TransUnion) and for you to be notified of key changes. You have ninety (90) days to activate this membership, which will then continue for 24 full months. Enrollment in this program will not hurt your credit score. We encourage you to activate your credit monitoring membership as soon as possible.*

The website to enroll in Triple Alert and your individual activation code are both listed below. To sign up, please visit the website and enter your individual activation code. Please keep in mind that once activated, the code cannot be re-used for another enrollment. The website will guide you through the process of enrolling in Triple Alert. If you need technical assistance, please call [insert Experian number].

Triple Alert Website: ***[insert URL]***
Your Activation Code: ***[insert activation code]***

If you wish to enroll over the phone for delivery of your membership via US Mail, please call 8xx-xxx-xxxx.]

Additional information about how to avoid identity theft is available through the Federal Trade Commission (http://www.ftc.gov/bcp/edu/microsites/idtheft/) and through your State Attorney General's Office.

Please accept our sincere apologies for this incident. We are committed to protecting confidential and personal information and have taken steps to avoid having this kind of incident happen again. Please contact me if you have any questions about this incident or need further information.

Sincerely,

Mary A. Beckman
Director of Compliance
tel: 857-218-4682

Note: Italicized text will appear only in letters to individuals whose social security number is involved.