LOSEY

Adam Losey
alosey@losey.law
407.906.1605

LOSEY PLLC
450 S. ORANGE AVE STE 500
ORLANDO, FL 32801

100 S. ASHLEY DR STE 600
TAMPA, FL 33602

524 E. COLLEGE AVE STE 100
TALLAHASSEE, FL 32301

www.losey.law

April 30, 2018

State of New Hampshire Department of Justice
Office of the Attorney General Joseph Foster
33 Capitol Street Concord, NH 03301

VIA U.S. MAIL

Pursuant to NH Rev Stat § 359-C:20, we are writing to notify you of a cybersecurity breach involving the personal information of residents of the State of New Hampshire on behalf of our client, The Children's Mercy Hospital ("Children's Mercy").

On December 2, 2017, the Children's Mercy information security team detected unauthorized account access to two email accounts associated with a phishing email sent to the two account holders, and these two accounts were reset by Children's Mercy's information security team the same day, December 2, 2017, to stop any unauthorized access. Two additional email accounts were also accessed by unauthorized persons on December 15 and 16 of 2017, and these accounts were reset by Children's Mercy's information security team on December 18, 2017 to stop any unauthorized access. Unauthorized access to an additional email account occurred on the night of January 3, 2018 and was detected by the Children's Mercy information security team on the morning of January 4, 2018; the account was reset on the morning of January 4, 2018 to stop the unauthorized access.

With the assistance of outside security experts, Children's Mercy's internal team investigated the incidents to determine what, if any, information was accessed. On January 19, 2018 Children's Mercy was able to determine that the mailbox accounts for four of the five affected individuals were downloaded by unauthorized individuals at the time of unauthorized access. Children's Mercy has reviewed and catalogued the information contained in the mailbox accounts to determine the identity and state of residence for those individuals affected. The review process is ongoing and due to the volume of information, a delay in breach notification has resulted. Additional remediation is in process, and Children's Mercy is continuing its investigation into the incident, taking steps to mitigate any impact to individuals, and to protect against any further incidents.

Although we are not aware of any misuse of patient information, we are notifying affected patients. The categories of information vary for individuals, but may have included first and last name, medical record number, gender, date of birth, age, height, weight, body mass index, admission date, discharge date, procedure date, diagnostic and procedure codes, clinical information, demographic information, diagnosis, conditions, other treatment information and identifying or contact information.

The number of New Hampshire residents affected is 2. These residents will receive notification of the data breach after April 30, 2018 via U.S. Mail by mailing made April 30, 2018.

At the present time, Children's Mercy is not aware of any misuse of the personal information of patients.

You may contact Robin V Foster, the Senior Vice President and General Counsel at Children's Mercy Hospital, at 2401 Gillham Road, Kansas City, Missouri, 64108, by phone at (816) 701-4510, or by e-mail at rvfoster@cmh.edu.

Please see the notice provided to the individuals impacted by the incident attached as **Exhibit A** to this letter.

Sincerely,

Adam Losey

Enclosures

Exhibit A – Notice to Individuals

Children's Mercy

Processing Center • P.O. BOX 141578 • Austin, TX 78714

00003 ACD1234

00048
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

April 30, 2018

Ref #: 1000124

Dear Valued Parent/Patient:

We are writing to inform you of an incident involving your or your child's personal information. On December 2, 2017, the Children's Mercy Information Security team detected unauthorized account access associated with a phishing email sent to two account holders. "Phishing" emails appear to be from a trusted source and often contain links to a phony login page on a fake website, frequently fabricating an urgent reason to motivate the recipient of the email to enter a username and password.

The two compromised accounts were reset by the Children's Mercy Information Security team the same day, December 2, 2017, to stop the unauthorized access. Two additional email accounts were also accessed by unauthorized persons on December 15 and 16 of 2017. These accounts were reset by the Children's Mercy Information Security team on December 18, 2017 to stop the unauthorized access. Unauthorized access to a fifth email account occurred on the night of January 3, 2018 and was detected by the Children's Mercy Information Security team on the morning of January 4, 2018. The account was reset on the morning of January 4, 2018. On January 19, 2018, Children's Mercy was able to determine that the mailbox accounts for four of the five affected employees were downloaded by unauthorized individuals at the time of unauthorized access.

With the assistance of outside security experts, Children's Mercy has been investigating to determine what contents were accessed in the email accounts during the periods of unauthorized access. We are notifying individuals as we continue to review the data at issue. Children's Mercy will continue to investigate the incident, take steps to mitigate any impact to individuals, and implement measures to protect against any further incidents.

Although we are not aware of any misuse of patient information, we are notifying potentially affected patients. The categories of information vary for individuals, but may have included first and last name, medical record number, gender, date of birth, age, height, weight, body mass index, admission date, discharge date, procedure date, diagnostic and procedure codes, clinical information, demographic information, diagnosis, conditions, other treatment information and identifying or contact information.

We want to make you aware of steps you may take to guard against identity theft or fraud. Please review the enclosed "How to Protect My Information," "Identity Theft – FTC Contact Information," and "AllClear Identity Repair Terms of Use." You can obtain information about fraud alerts and security freezes from the sources indicated in these attachments.

You may obtain additional information about how to avoid identity theft from the Federal Trade Commission or your state attorney general. You also have the right to file or obtain a police report. We advise that you report any suspected identity theft incidents to local law enforcement, the Federal Trade Commission, or your state attorney general. Also, enclosed are toll-free numbers and addresses for consumer reporting agencies and the Federal Trade Commission. You may also obtain information from these sources about fraud alerts and security freezes.

01-04-3-00

As a precautionary measure, we also recommend that you remain vigilant for fraud and identity theft by reviewing your account statements and free credit reports closely to detect errors resulting from this incident. As an added precaution, we have arranged to have AllClear ID protect your/your child's identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available with no enrollment required. If a problem arises, simply call 1-855-354-4116 and a dedicated investigator will help recover financial losses, restore credit and make sure your/your child's identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of fraud against children by searching thousands of public databases for use of your child's information. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-354-4116 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

If you wish to speak to someone concerning this matter please call our dedicated assistance line, Monday through Saturday, 8 am – 8 pm CT, at:

1-855-354-4116

Information may also be found at childrensmercy.org/February2018.

You also have the right to file a complaint with the Department of Health and Human Services, Office of Civil Rights, Region VII. To do so, go to: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html. For additional information on how to protect your personal information, please see the attached information entitled "How to Protect My Information."

For residents of Maryland, please note that the following contact information for the Office of the Maryland Attorney General may be used to obtain additional information about how to avoid identity theft. The attorney general's office may be reached, toll-free, at 1-888-743-0023. You may also visit the Office of the Maryland Attorney General at the address below or online at the website below.

Brian E. Frosh, Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

http://www.marylandattorneygeneral.gov/

For residents of New Mexico, please note that under Chapter 56, Article 3A of the New Mexico Code, otherwise known as the Fair Credit Reporting and Identity Security Act, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal.

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;
(2) proper identification to verify your identity;
(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
(4) payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act." NM Stat. § 56-3A-4 (2016).

For residents of North Carolina, please note that the following contact information for the North Carolina Attorney General's Office may be used to obtain additional information about preventing identity theft. The attorney general's office may be reached, toll-free, at 1-877-5-NO-SCAM (1-877-566-7226). You may also visit the North Carolina Attorney General's Office at the address below or online at the website below.

Josh Stein, North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001

http://www.ncdoj.gov/Home.aspx?lang=en-US

For residents of Wisconsin, please note that upon your written request to the contact information provided in this letter, Children's Mercy will identify the personal information pertaining to you that was accessed and acquired by the unauthorized party mentioned above.

Children's Mercy takes the protection of personal information seriously. We have taken and will continue to take steps to prevent any such incidents involving personal information, including re-education and re-training of key staff on internet scams such as phishing emails. These steps are in addition to our mandatory ongoing education for all employees regarding data security and privacy.

Please accept our deepest apologies for this incident. We sincerely regret any inconvenience or concern this has caused.

Sincerely,

Shelli Crocker

Shelli Crocker, MA, CISSP
Information Security Compliance Officer Corporate Compliance
Children's Mercy Kansas City
2401 Gillham Road
Kansas City, MO 64108

How to Protect My Information

State law allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any request you make for new loans, credit, credit or debit cards, mortgages, employment, housing or other services.

If at any time you become a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

Credit Report Security Freeze Instructions

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
1-800-349-9960

TransUnion Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
1-800-680-7289

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 victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, a payment of $5.00 by check, money order, or credit card (Visa, MasterCard, American Express or Discover only) for the freeze. Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security 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 lift the security freeze in order to allow a specific entity or individual to access 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 lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus 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. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Identity Theft — FTC Contact Information

The Federal Trade Commission is located at 600 Pennsylvania Avenue, NW Washington, DC 20580. If you believe you may have been a victim of identity theft, you may file a complaint with the Federal Trade Commission at: www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338).

Here are a few warning signs to help you determine that whether your personal information may have been used by someone else:

- Receiving a bill for services you did not purchase or receive never used
- Being contacted by a debt collector about debt you do not owe
- Seeing collection notices on your credit report that you do not recognize

If you believe someone else may have used your information, you may wish to consider taking additional steps which are outlined on the Federal Trade Commission's website at www.ftc.gov.

AllClear Identity Repair 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:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair 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 Identity Repair 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

Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements

To be eligible for Services under AllClear Identity Repair 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, 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 Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair 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; and
- 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 Identity Repair 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, or
  - 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; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair 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 Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- 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.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, 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