ROTECH HEALTHCARE INC.

We Care About Patient Care

October 24, 2013

Office of the Attorney General
NH Department of Justice
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

As you are aware, New Hampshire state law requires notice to the New Hampshire Attorney General in the event of an information security breach involving the personal information of New Hampshire residents. In accordance with that requirement, I write to inform you of an information security breach. Within the last week, we matched all the compromised personal information, to the extent we reasonably could, with addresses resulting in a list of all of the states of residents of the affected individuals. New Hampshire is one of the states in which affected individuals reside.

On August 30, 2013, we were informed that a former employee had removed certain files from our premises when the employee stopped working at Rotech on November 26, 2010. These files contained personal information regarding Rotech employees and their dependents. The personal information that was removed may have included names, addresses, social security numbers, the name of one or more of the carrier(s) that administered the resident's health care coverage, and/or limited information about certain medical or pharmacy services the resident received. Our former employee appears to have removed this personal information inadvertently. She has deleted all personal information from the device on which this information was stored, and is returning the device to us.

To date, we have no evidence or information that anyone's personal information has been or will be misused. In response to this incident, we are reviewing and enhancing our information security practices and procedures to reduce the risk that someone can take electronic files containing personal information away from our premises. We are also providing additional training to all employees with access to personal information to remind them of their obligations to safeguard it and to keep it confidential. In addition to these protections, we are undertaking a thorough review of our document access and data loss processes to determine if there are additional measures we can take in our effort to prevent an incident like this from occurring again.

We believe that approximately 20 New Hampshire residents were affected by this incident. On October 24, 2013 we began mailing written notifications to all affected New Hampshire residents. As a precaution, we offered complimentary credit monitoring services to those residents whose social security number may have been compromised and provided everyone other precautionary information and measures they can take to

safeguard their identities. For your convenience, a copy of the notice template being sent to affected New Hampshire residents is enclosed with this letter.

If you have any questions or need further information regarding this incident, please do not hesitate to contact me.

Sincerely,

Robin L. Menchen

Robin L. Menchen
Chief Privacy Officer

October 24, 2013 FORM 1

Dear [Insert Name and Address]:

We recently learned that a former Rotech employee who, as part of the employee's job responsibilities, had access to electronic files containing personal information of Rotech employees and their dependents ("Personal Information"), took certain of these electronic files upon resigning from Rotech on or about November 26, 2010. The former employee has advised us that the removal of Personal Information was inadvertent, and incidental to the removal of other electronic general workplace files for the employee's future use. This person's next employer notified us on August 30, 2013, that they discovered files containing Personal Information on the non-networked computer this person had used at their office. They sent the electronic files containing Personal Information to us, and also confirmed to us that they destroyed all Personal Information whatsoever that resided on the personal computer this person used at their office. Subsequently, we determined what Personal Information our former employee had taken.

We are writing to inform you that the files this employee removed included Personal Information about you from our medical plan; specifically, they included your name, address, social security number, the name of one or more of the carrier(s) that administered your health care coverage, and limited information about certain medical or pharmacy services you received.

At this time, we have no evidence that your Personal Information has been or will be misused in any way. We interviewed the former employee, who expressed surprise that Personal Information was included in the work files removed from our office. The former employee assured us that none of the Personal Information ever was accessed or used for any purpose while it was stored out of our office. The former employee also told us that all copies of Rotech files, including the files on the external device to which the Personal Information was downloaded and stored, have been deleted, and the device will be handed over to us.

Please see the enclosure entitled "Important Steps to Prevent Fraud" to learn more about services and precautions you can take to protect yourself against the possibility of becoming a victim of identity theft. To help you protect your identity, we are offering a complimentary one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. Your Activation Code is: **[code]** Activation steps and additional details are enclosed.

Even if you choose not to enroll in the free credit monitoring service, we encourage you to actively monitor your financial accounts and the free credit reports that are available to you. You should report any identity theft you suspect may be related to this incident to appropriate law enforcement officials and to the following toll-free number: (866) 686-8704.

Please be assured that we take the privacy of your personal information very seriously. In response to this incident, we are reviewing and enhancing our information security practices and procedures to reduce the risk that someone can take electronic files containing Personal Information away from our premises. We are also providing additional training to all employees with access to Personal Information to remind them of their obligations to safeguard it and to keep it confidential. In addition to these protections, we are undertaking a thorough review of our document access and data loss processes to determine if there are additional measures we can take in our effort to prevent an incident like this from occurring again.

We sincerely apologize for this incident and regret any inconvenience it may cause you. If you have any questions about this incident, please contact the toll-free number we have set up for this purpose, which is (866) 686-8704.

Sincerely,

Robin L. Menchen
Chief Privacy Officer

Important Steps to Prevent Fraud

For residents of *California, Hawaii, Illinois, Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, Vermont, Virginia, West Virginia,* and *Wyoming*:

It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account by contacting any one or more of the national consumer reporting agencies listed below. They can also provide you with information about fraud alerts and security freezes.

Equifax
P.O. Box 740241
Atlanta, GA 30348
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2104
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 6790
Fullerton, CA 92834-6790
1-877-322-8228
www.transunion.com

For residents of *Iowa*:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of *Illinois, Maryland* and *North Carolina*:

State laws require us to tell you that you can obtain information from the Federal Trade Commission about steps you can take to avoid identity theft (including how to place a fraud alert or security freeze). If you are a Maryland or North Carolina resident, you may also be able to obtain this information from your state's Attorney General.

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

NC Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
http://www.ncdoj.gov/

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

For residents of *Massachusetts* and *West Virginia*:

State laws require us to inform you of your right to obtain a police report if you are a victim of identity theft. You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit.

To place a security freeze on your credit report, you need to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 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 you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

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

TransUnion (FVAD)
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

What we are doing to protect your information:

To help protect your identity, we are offering a **complimentary** one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: January 31, 2014** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/redeem**
3. PROVIDE **Your Activation Code**

If you have questions or need an alternative to enrolling online, please call 877-371-7902.

ADDITIONAL DETAILS REGARDING YOUR {12-MONTH} PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-371-7902.

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.