ROTECH
HEALTHCARE INC.

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

00001
ACD1234

00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

August 8, 2016

Dear John Sample,

Rotech Healthcare, Inc. ("Rotech") is writing to notify you of a recent incident that may affect the security of your personal and protected health information. In this letter, we are providing you with information regarding the incident, steps we have taken since discovering the incident, and what you can do to better protect against the possibility of identity theft and fraud should you feel it is appropriate to do so.

Who is Rotech? Rotech provides health care services, including home medical equipment and supplies, to our patients directly and through our subsidiary companies. You are receiving this letter because you have received services from Rotech or one of our subsidiary companies in the past.

What Happened? On June 13, 2016, Rotech received a report that certain patient information had been recovered by law enforcement after being found in the possession of an unauthorized individual. After receiving this report, Rotech immediately launched an investigation to verify the information provided and to learn more about what may have happened. Third party forensic investigators have been retained to assist with the investigation into what happened, the identification of what information may be at risk and to whom this information relates. On July 11, 2016, the United States Secret Service provided Rotech with copies of the patient information that had been recovered. A review of the recovered records indicates the records did come from Rotech systems.

What Information Was Involved? Although the investigations into this incident by Rotech and law enforcement are ongoing, Rotech determined that the paper records recovered by law enforcement contained your personal and protected health information, including the following: name, Social Security number, patient number, address, the name of the Rotech subsidiary company from which you received health care services, and possibly phone number and/or date of birth.

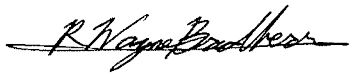
What We Are Doing. Rotech takes your privacy and the security of your personal and protected health information very seriously, and we are cooperating with law enforcement's investigation into this incident. Rotech and our third party forensic investigators continue to investigate this incident to identify any additional patients who may be impacted by this incident. We are providing notice to all patients whose information was provided to Rotech by law enforcement and will be notifying any additional impacted individuals as they are identified. As part of our ongoing commitment to the security of the information in our care, we are reviewing our existing policies and procedures to better prevent something similar from happening again. We are notifying the Department of Health and Human Services and certain state regulators about this incident.

We are also offering you access to a complimentary 24-month membership to credit monitoring and identity protection services through AllClear ID. The enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud* includes more information on these services and instructions on how to enroll and receive them.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud.* There you will find guidance on how to better protect against the possibility of identity theft and fraud. The complimentary credit monitoring and identity protection services are available to you, should you wish to enroll to receive them. We know you may have questions about the content of this letter and have established a confidential, toll-free hotline to assist you with these questions and the steps you can take to better protect against the possibility of identity theft and fraud. The hotline is available Monday through Saturday, 9:00 a.m. to 9:00 p.m., EST, at 1-855-269-6650.

We sincerely regret any inconvenience this incident may cause. Rotech remains committed to safeguarding information in our care and will continue to take proactive steps to enhance the security of the information in our care.

Sincerely,



R. Wayne Bradberry, CHC
Vice President, Compliance and Ethics

Steps You Can Take to Protect Against Identity Theft and Fraud

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 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 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-269-6650 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use 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 1-855-269-6650 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

In addition to enrolling and receiving the above services, you may also take action directly to further protect against possible identity theft or financial loss. We encourage you to remain vigilant against incidents of identity theft and fraud and seek to protect against possible identity theft or other financial loss by regularly reviewing your financial account statements for any charges you did not make. We also encourage you to notify your financial institutions and health care insurers of this data security event to seek advice regarding protecting your accounts.

We encourage you to regularly review any Explanation of Benefits statements 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 your statement. If you do not receive regular Explanation of Benefits statements, you can contact your insurer and request that they send such statements following the provision of services in your name or number. You may also want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, you can call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.

We also suggest that you carefully review your credit reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, you may visit www.annualcreditreport.com, or call, toll-free, (877) 322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. When you receive your credit reports, they should be reviewed carefully. You are encouraged to look for accounts you did not open as well as inquiries from creditors that you did not initiate. Also, you should look for personal information that is not accurate, such as home address or Social Security number. If you see anything on the report that you do not understand, call the credit reporting agency at the telephone number on the report. If you find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. You should ask for a copy of the police report, as you may need to give copies of the police report to creditors to clear your records. Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports periodically.

At no charge, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Please note, however, that because it tells creditors to follow certain procedures to protect an individual's credit, it may also delay the ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms a fraud alert, the others are notified to place fraud alerts on your file. If you wish to place a fraud alert, or you have questions regarding your credit report, you can contact any one of the following agencies:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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.

If you are the victim of identity theft, and provide the credit bureau with a valid police report, you will not be charged to place, lift or remove a security freeze. In other cases, a credit bureau may charge a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place the freeze on all of their credit files.

For more information on how to place a security freeze, affected individuals may use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	888-909-8872
www.equifax.com/help/credit-freeze/en_cp	www.experian.com/freeze/center.html	www.transunion.com/freeze

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect themselves, by contacting your state Attorney General or the Federal Trade Commission (FTC). The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. You should also report known or suspected identity theft to your state Attorney General or local law enforcement. Your state Attorney General may have advice on preventing identity theft. You can also learn more about placing a fraud alert or security freeze on your credit files by contacting the FTC or your state Attorney General.

Data Breach Notification

Rotech Healthcare Inc. ("Rotech") would like to notify you of a recent incident that may affect the security of your personal and protected health information. We are providing you with information regarding the incident, steps we have taken since discovering the incident and what you can do to protect against the possibility of identity theft and fraud should you feel it is appropriate to do so.

What Happened?

On June 13, 2016, Rotech received a report that certain patient information had been recovered by law enforcement after being found in the possession of an unauthorized individual. After receiving this report, Rotech immediately launched an investigation to verify the information provided and to learn more about what may have happened. Third-party forensic investigators were retained to assist with the investigation into what happened, the identification of what information may be at risk and to whom this information relates. On July 11, 2016, the United States Secret Service provided Rotech with copies of the patient information recovered. A review of the recovered records indicates the records came from Rotech systems.

What Information Was Involved?

Although the investigations into this incident by Rotech and law enforcement are ongoing, Rotech determined that the paper records recovered by law enforcement contained your personal and protected health information, including : name, Social Security number, patient number, address, the name of the Rotech subsidiary company from which you received health care services, and possibly phone number and/or date of birth.

What We Are Doing?

Rotech takes your privacy and the security of your personal and protected health information very seriously, and we are cooperating with law enforcement's investigation into this incident. Rotech and our third party forensic investigators continue to investigate this incident to identify any additional patients who may be impacted by this incident. We are providing notice to all patients whose information was provided to Rotech by law enforcement and will notify any additional impacted individuals as they are identified. As part of our ongoing commitment to the security of the information in our care, we are reviewing our existing policies and procedures to better prevent something similar from happening again. We are notifying the Department of Health and Human Services and certain state regulators about this incident.

What You Can Do.

You can review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*. There you will find guidance on how to better protect against the possibility of identity theft and fraud. We know you may have questions about the content of this letter and have established a confidential, toll-free hotline to assist you with these questions and the steps you can take to better protect against the possibility of identity theft and fraud. The hotline is available Monday through Saturday, 9:00 a.m. to 9:00 p.m., EST, at 1-855-269-6650.

We sincerely regret any inconvenience this incident may cause. Rotech remains committed to safeguarding information in our care and will continue to take proactive steps to enhance the security of the information in our care.

Sincerely,

R. Wayne Bradberry, CHC
Vice President, Compliance & Ethics

Data Breach Notification

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud and seek to protect against possible identity theft or other financial loss by regularly reviewing your financial account statements for any charges you did not make. We also encourage you to notify your financial institutions and health care insurers of this data security event to seek advice regarding protecting your accounts.

We encourage you to review any Explanation of Benefits statements 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 your statement. If you do not receive regular Explanation of Benefits statements, you can contact your insurer and request that they send such statements following the provision of services in your name or number. You may also want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, you can call the credit-reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.

We also suggest that you carefully review your credit reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, you may visit www.annualcreditreport.com, or call, toll-free, (877) 322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. When you receive your credit reports, they should be reviewed carefully. You are encouraged to look for accounts you did not open as well as inquiries from creditors that you did not initiate. In addition, you should look for personal information that is not accurate, such as home address or Social Security number. If you see anything on the report that you do not understand, call the credit-reporting agency at the telephone number on the report. If you find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. You should ask for a copy of the police report, as you may need to give copies of the police report to creditors to clear your records. Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports periodically.

At no charge, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Please note, however, that because it tells creditors to follow certain procedures to protect an individual's credit, it may also delay the ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms a fraud alert, the others are notified to place fraud alerts on your file. If you wish to place a fraud alert, or you have questions regarding your credit report, you can contact any one of the following agencies:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA30348	Allen, TX 75013	Chester, PA19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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.

If you are the victim of identity theft, and provide the credit bureau with a valid police report, you will not be charged to place, lift or remove a security freeze. In other cases, a credit bureau may charge a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place the freeze on all of their credit files.

For more information on how to place a security freeze, affected individuals may use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-685-1111	888-397-3742	888-909-8872
www.equifax.com/help/credit-freeze/en_cp	www.experian.com/freeze/center.html	www.transunion.com/freeze

You can further educate yourself regarding identity theft, fraud alerts, security freezes and the steps you can take to protect themselves, by contacting your state Attorney General or the Federal Trade Commission (FTC). The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft ; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1- 866-653-4261. You should also report known or suspected identity theft to your state Attorney General or local law enforcement. Your state Attorney General may have advice on preventing identity theft. You can also learn more about placing a fraud alert or security freeze on your credit files by contacting the FTC or your state Attorney General.