SIDLEY AUSTIN LLP

SIDLEY

[redacted]

BEIJING
BOSTON
BRUSSELS
CHICAGO
DALLAS
FRANKFURT
GENEVA
HONG KONG
HOUSTON
LONDON
LOS ANGELES
NEW YORK
PALO ALTO
SAN FRANCISCO
SHANGHAI
SINGAPORE
SYDNEY
TOKYO
WASHINGTON, D.C.

FOUNDED 1866

March 2, 2015

By FedEx and Email

The Honorable Attorney General Joseph Foster
New Hampshire Department of Justice
33 Capitol St.
Concord, NH 03301
[redacted]

Dear General Foster:

We write on behalf of our client, Amedisys, Inc. ("Amedisys") to notify you under your state data breach law.

During the second half of 2014, Amedisys began an extensive risk management process to verify its large inventory of clinical and non-clinical computers which contain personal and healthcare information of patients. As of February 23, 2015, Amedisys could not rule out unauthorized access to patient data on approximately 142 computers and laptops.

These computers and laptops housed patient information, which, depending on the device, includes name, address, Social Security numbers, date of birth, Medicare and insurance numbers, medical records and other personally identifiable information. For clinician laptops, these records related only to those patients assigned to the clinicians who used a device to provide healthcare services. Amedisys robustly protects its devices with 256-bit disk encryption, administrator restrictions, and several other security protections designed to safeguard the personal and medical information of the Company's patients. Former employees, however, had access to the encryption key for local access to their formerly assigned device, although Amedisys disabled their network password.

Starting on February 28, 2015, Amedisys began sending notification letters to the approximately 31 New Hampshire residents whose personal and medical information may have been affected by this incident. Although Amedisys has no evidence that any patient's information was inappropriately used, out of an abundance of caution, the Company is offering free credit monitoring and identity theft protection services to potentially affected patients, as described in the attached notice template enclosed with this letter. A sample notification letter sent to potentially affected New Hampshire residents is enclosed herein.

Amedisys, Inc. is submitting this letter on behalf of itself and several of its subsidiaries, some of which do business under other names and in multiple locations. We would be happy to provide supplemental information about corporate structure as requested.

In response to this incident, Amedisys has committed to improving the way it tracks devices to ensure it maintains an updated device inventory, reinforcing existing policies and practices and implementing additional safeguards.

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

Sincerely,

[redacted]

<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<Address1>>
<Address2>>
<<City>>, <<State>> <<Zip Code>>

February 28, 2015

Dear <<MemberFirstName>> <<MemberLastName>>,

Amedisys, Inc. ("Amedisys"), the parent company that owns your home healthcare provider, is writing to notify you of a breach under applicable data privacy laws involving your personal and medical information. Please be assured that we take your privacy and the confidentiality of your personal and medical information very seriously. We have taken many steps, as described in this letter, to prevent harm to you as a result of this situation and are working to avoid an issue like this in the future.

Situation

An Amedisys inventory has shown that a laptop or computer used in connection with the home healthcare Amedisys provided to you has not been located within the Amedisys system. Our records indicate that this device was originally assigned to a licensed clinician or other Amedisys team member as of <<ClientDef1 (Date)>>. The computer at issue contained your medical records, including Social Security number, date of birth and Medicaid/Medicare number.

There is no evidence that your information was inappropriately used, and we have received no reports of any hacking, fraud, or identity theft. However, as required by law and out of an abundance of caution for our patients, we are providing notice to all patients whose information was on devices that we have not been able to reconcile as of the February 23, 2015 completion of our inventory process.

Our Commitment to You

In an effort to ensure that no patient can be harmed by this incident, we are offering you one year of credit monitoring and identity protection services through Kroll. You can sign up for these services by visiting Kroll's website at **kroll.idMonitoringService.com**, and following the online instructions to activate your "Identity Theft Protection" package. Some Kroll services are only available online. You may call Kroll at **1-855-205-6937** if you have any questions. **Your membership number is** <<Member ID>>.

As a further precaution, we recommend that you monitor your tax returns, health benefit statements, credit card and other financial statements. If you notice any unusual activity, please notify your financial institution immediately.

We are committed to protecting the privacy and security of our patients' medical and personal information. Our computers are robustly protected with 256-bit disk encryption, administrator restrictions and a number of other security protections designed to safeguard the personal and medical information of our patients. In order to ensure Amedisys has an updated inventory of its devices, we are improving the way we track devices, reinforcing existing policies and practices, and implementing additional safeguards.

Additional Information

We understand you may have additional questions about what this means for you. In order to answer questions, we have established a website at www.Amedisys.com/Security and a toll-free hotline at **1-855-205-6937**. Representatives are available between the hours of 9:00 am to 6:00 pm Eastern Standard Time.

Please accept our deepest apologies for any inconvenience. We are grateful to our patients and their families for the trust they place in Amedisys as we work to advance care in our communities.

Sincerely,

Jeffrey Jeter
Chief Compliance Officer
Amedisys, Inc.

kroll.idMonitoringService.com is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with yoiur credit file. To receive credit services by mail instead of online, please call 1-855-205-6937.

Take Advantage of Your Identity Theft Protection Services

You've been provided with access to services from Kroll, a global leader in risk mitigation. Over the past 14 years, Kroll has provided data breach response services for cases impacting more than 100 million individuals including personal consultation to more than 180,000 consumers and worked some 8,000 confirmed identity theft cases. When you need assistance, rest assured that your services are backed by an expert team who can answer any question you may have.

The following services are included in your **Essential Monitoring** package:

Kroll employs a team of experienced licensed investigators to provide you with expert, one-on-one assistance:

Consultation: You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes best practice tips to assist in ongoing protection, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Restoration: Kroll's restoration services are the most comprehensive of any provider. Should you become a victim of identity theft, a dedicated licensed investigator can work on your behalf to resolve related issues. The investigator does more than shoulder the bulk of the recovery; they can dig deep to uncover all aspects of the theft, and then work with creditors, collection agencies, utilities, government entities, and more … to resolve it.

Credit Monitoring through TransUnion: Credit services can be a key tool in detecting early warning signs of identity theft. You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll investigator, who can help you determine if it's an indicator of identity theft. You'll also receive "no activity" notices if there have been no changes to your data.

Web Watcher: Web Watcher helps to detect if your personal information is being bought and sold online. This program monitors hacker chat rooms, forums and other websites where criminals are known to trade stolen information. Thousands of sites are monitored, looking for matches to your personal information, such as Social Security, medical ID, and financial account numbers. If your information is found, you will be promptly alerted and provided with instructions to contact your investigator. Monitoring starts as soon as you enroll and select the information to search.

Your identity theft protection services are continued on back …

How to Take Advantage of Your Identity Theft Protection Services

Visit kroll.idMonitoringService.com

and follow the online instructions to take advantage of your identity theft protection services.

You can view your services at any time by logging onto Kroll's identity protection website. When you enroll, be prepared to provide the membership number included with the accompanying letter.

Help is only a phone call away.

If you have a question, need assistance, or feel you may be a victim of identity theft, call Kroll at the toll-free number provided in the accompanying letter, and ask to speak with an investigator

Take advantage of this no-cost opportunity and let the experts at Kroll help you assess your situation and safeguard your identity.

Kroll.idMonitoringService.com is compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox or Safari.

Public Persona: Public Persona monitors public record databases for names, aliases and addresses that are associated with your Social Security number. Records include, among other data sources, property or deed registration, internet job site providers, state occupational license data, and court proceedings. If information is found, an alert email is sent. If you see a name, address or alias that is not associated with you, contact Kroll's investigators for more information. Once you have enrolled, you can view the services at any time by logging onto Kroll's identity protection website.

Quick Cash Scan: Quick Cash Scan monitors thousands of short-term and cash-advance loan sources, such as rent-to-own or payday lenders. These are sometimes referred to as "non-credit" loans because the application process does not always include a credit check, making it easier to use stolen or fraudulent identity information. You'll receive an alert when a loan is reported, and you'll have the option to call a Kroll investigator for more information.

$1 Million Identity Theft Insurance: Reimburses you for out-of-pocket expenses totaling up to $1 million in legal costs for any one stolen identity event. Additional benefits include a $0 deductible and coverage for fees associated with replacing documents, traveling expenses, loss of income, child care and elderly care and fraudulent withdrawals. All coverage is subject to the conditions and exclusions in the policy.

State Notification Requirements

All States.
You may obtain a copy of your credit report or request information on how to place a fraud alert or security freeze by contacting any of the national credit bureaus below. It is recommended 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.

Equifax
P.O. Box 740241
Atlanta, GA 30374
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 2000
Chester, PA 19022
1-800 -888-4213
www.transunion.com

For residents of Massachusetts.
It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Massachusetts and West Virginia.
You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above.
A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent.
To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. 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 and free if 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.

For residents of Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, and West Virginia.
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

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.
You can obtain information from the Federal Trade Commission, and for residents of Maryland and North Carolina, from your respective state Office of the Attorney General, about steps you can take toward preventing identity theft.

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/

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

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699 -9001
1-877-566 -7226
www.ncdoj.com