



MULLEN
COUGHLIN

STATE OF NH
DEPT OF JUSTICE

2016 OCT 24 PM 12:01

Christopher J. DiIenno
Office: 267-930-4775
Fax: 267-930-4771
Email: cdiienzo@mullen.legal

1275 Drummers Lane, Suite 302
Wayne, PA 19087

October 20, 2016

VIA U.S. FIRST CLASS MAIL

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Cyber Security Incident

Dear Attorney General Foster:

We represent Apria Healthcare, 26220 Enterprise Court, Lake Forest, CA 92630, and are writing to notify you of a cyber security incident that may affect the security of the personal information of three (3) New Hampshire residents. The investigation into this incident is ongoing and will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Apria Healthcare does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Cyber Security Incident

Apria Healthcare is one of the nation's leading providers of home respiratory services and certain medical equipment. On August 5, 2016, Apria Healthcare discovered that the email account of an Apria Healthcare employee was subject to unauthorized access and immediately launched an internal investigation and retained third-party forensic experts to assist in the investigation of the incident. The employee's log-in credentials were changed and the security of the system was restored. The forensic investigators later determined that (i) there was no evidence that data was exfiltrated, (2) other than the one employee's email account, no other aspect of Apria's system was compromised, and (iii) the email account contained the personal information of certain individuals. Apria Healthcare then undertook a thorough analysis and review of all documents within the email account to determine all affected individuals and data types involved.

Attorney General Joseph Foster
October 20, 2016
Page 2

The data potentially subject to unauthorized access includes a combination of name, date of birth, patient identification number, Social Security number, diagnosis information, doctor's name, type of medical equipment requested, treatment location, medical record number, driver's license or state identification number and/or health insurance information.

Notice to New Hampshire Residents

Once Apria Healthcare identified all individuals impacted by this incident, an investigation was undertaken to determine the most current address for each impacted individual so that written notice of the incident could be provided to each one. On October 4, 2016, Apria Healthcare began mailing notice letters to impacted members which includes three (3) New Hampshire residents of which none had their Social Security number potentially exposed. The notice was provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and to Be Taken

Apria Healthcare is offering potentially affected individuals complimentary access to twelve (12) months of free credit monitoring and identity restoration services with AllClear ID. Additionally, Apria Healthcare is providing potentially affected individuals with information on how to protect against identity theft and fraud, including information on how to contact the Federal Trade Commission, the state attorney general, and law enforcement to report any attempted or actual identity theft and fraud. In addition to providing notice of this incident to you, Apria Healthcare is providing written notice of this incident to other state regulators where required.

Contact Information

Should you have any questions regarding this notification or other aspects of the cyber security incident, please contact me at 267-930-4775.

Very truly yours,



Chris J. DiIenno of
MULLEN COUGHLIN LLC

CJD:ncl
Enclosure

Exhibit A



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



00018
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

October 20, 2016

RE: Notice of Data Breach

Dear John Sample:

Apria Healthcare recently discovered an incident that may affect the security of your personal information. Apria Healthcare is one of the nation's leading providers of home respiratory services and certain medical equipment. You may have received certain medical equipment from Apria Healthcare. We write to provide you with information about the incident, steps taken since discovering the incident, and information on what you can do to better protect against the possibility of identity theft and fraud.

What Happened? On August 5, 2016, we discovered that the email account of an Apria Healthcare employee was subject to unauthorized access. We immediately launched an internal investigation and retained third-party forensic experts to assist in the investigation of the incident. The forensic investigators later determined that the email account contained the personal information of certain individuals, including you. We then undertook a thorough analysis and review of all documents within the email accounts to determine all affected individuals and data types involved.

What Information Was Involved? We determined that while the unauthorized individual or individuals had access to the employee's email account, certain of your personal information may have been viewed by the unauthorized individual including demographic information such as your name and/or date of birth, and certain of your medical information which may include patient number, diagnosis information, type of treatment or product received, medical record number and Client DEF 1.

What We Are Doing. We take this incident and the security of your personal information very seriously. In addition to notifying individuals potentially impacted by this incident, we are offering you complimentary access to twelve (12) months of free credit monitoring and identity restoration services with AllClear ID. The enclosed *Other Important Information* contains instructions on how to enroll and receive these free services, as well as more information on how to better protect against identity theft and fraud. We are also notifying certain federal and state regulators of this incident.

What You Can Do. We encourage you to consider enrolling to receive the free credit monitoring and identity restoration services and review the information regarding how you can protect yourself found in the enclosed *Other Important Information* sheet.

For More Information. Please contact the confidential call center we've established regarding this incident. The call center is staffed with professionals who can answer questions about this incident and give you information on how to protect against misuse of your information. The call center is available Monday through Saturday, 8 a.m. to 8 p.m. Central Time at 1-855-303-6661.



01-02-2-00

We take the privacy of your personal information seriously. We sincerely regret any inconvenience or concern this incident has caused you. The security of your information is a priority to us and we have taken precautionary measures to mitigate the risk of any future reoccurrence.

Sincerely,

A handwritten signature in black ink, appearing to read "D. R. B.", with a stylized flourish at the end.

Doreen Bellucci
Vice President and Associate General Counsel

OTHER IMPORTANT INFORMATION

While we continue to investigate the incident, you may take action directly to further protect against possible identity theft or financial loss.

To help detect the possible misuse of your information, we are providing you with 12 months of free access to credit monitoring and identity restoration services with AllClear ID. 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 to you with no enrollment required. If a problem arises, simply call 1-855-303-6661 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 1-855-303-6661 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.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also 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. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289
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 have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, list or remove a security freeze. In all other cases, a credit bureau may charge you 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 a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
(NY residents please call
1-800-349-9960)
www.equifax.com/help/credit-freeze/en_cp

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
PO Box 2000
Chester, PA 19022-2000
1-888-909-8872
www.transunion.com/securityfreeze



You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. Notice has not been delayed due to a law enforcement investigation.