APRIA HEALTHCARE

26220 Enterprise Court
Lake Forest, California 92630
Tel 949.639.2000

September 27, 2012

Attorney General Michael Delaney
New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Security Incident

Dear Mr. Delaney:

This letter is to provide an update regarding a security breach incident with respect to which we provided notification to your office on August 15, 2012 ("Incident"). A copy of the August 15 notice is attached for your reference.

After we notified your office about the Incident, our digital forensics experts continued to sort through thousands of duplicative files that are believed to be on the laptop's hard drive. Using state-of-the-art software, our experts performed this data analysis in multiple phases because of the sheer volume of the data involved and certain technical issues encountered by them. The data forensics analysis was recently completed, and it was determined that an additional 116 individuals who are believed to be Indiana residents (based on the last address on file with us) were affected by the Incident. Therefore, based on the last address we have on file with us for each individual, we believe the total of the affected New Hampshire residents is 121.

Notices to these additional affected residents will be mailed out in waves within the next ten (10) business days or so. A copy of a sample letter is attached.

If you have any questions, I may be reached at 949-639-4141 to discuss this matter.

Very truly yours,

Ako S. Williams
Assistant General Counsel

Enclosures

APRIA HEALTHCARE

26220 Enterprise Court
Lake Forest, CA 92630

September 28, 2012

Sample A. Sample
123 Anystreet
Anytown, US 12345-6789

Important: Health Information Security and Protection Notification

This is **official correspondence from Apria Healthcare, Inc.** (Apria) to inform you of a data security incident. On June 14, 2012, a laptop with password protection and owned by Apria was stolen from an employee's locked vehicle. Since that time, we have been investigating the incident thoroughly with the help of legal, computer, and compliance experts. Unfortunately, we learned that the files on the stolen laptop contained some of our current and past patients' personal information that was given to us as part of providing homecare equipment or service. We recently discovered that this may include your Social Security Number (SSN) and name, and may have included your date of birth and/or other personal or health information. We truly regret that this incident occurred and understand that it may concern you.

While we have no reason to believe that the information has been used by an inappropriate party, we have taken many steps to address the incident and are committed to fully protecting all of your personal information. To prevent this type of incident from happening again, we are retraining our employees, changing certain data storage policies and exploring new technologies to further protect company data.

To help you monitor the situation, Apria is providing **free** coverage by Experian's ProtectMyID™ Alert program for one year. This product helps detect possible misuse of your personal information and provides you with superior identity protection services. Once your ProtectMyID membership is activated, your credit report will be monitored daily for 50 leading indicators of identity theft. You'll receive periodic Credit Alerts from ProtectMyID on any key changes in your credit report.

In the unlikely case that identity theft is detected, ProtectMyID will assign a dedicated U.S.-based Identity Theft Resolution Agent who will walk you through the process of fraud resolution from start to finish.

Activate Your Free ProtectMyID Service now in Three Easy Steps:

1. **ENROLL** by November 30, 2012
2. **VISIT** the ProtectMyID Web Site: http://www.protectmyid.com/redeem or **CALL** 888-451-6562 to enroll
3. **PROVIDE** Your Personal Activation Code: 999999999

For added protection, once you enroll, you will receive ExtendCARE™, which provides you with the same high level of Fraud Resolution support even after your ProtectMyID membership has expired after one year, at no additional cost to you.

Activate your membership today at http://www.protectmyid.com/redeem or call 888-451-6562 to register with the activation code found on page 1.

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 your credit report, or suspect that an item on it may be fraudulent, please contact Experian's customer care team at 888-451-6562.** Please note that you will be asked to provide your SSN in order to confirm your identity and enroll you in the program.

Other steps you may take include:

Checking your credit and similar accounts frequently over the next few years.

Notifying one of the three national credit reporting agencies to place a fraud alert, which will aid in preventing new credit accounts from being opened without your permission:

Credit Reporting Agency	Telephone Number	Website	Postal Address
Equifax	1-800-685-1111	www.equifax.com	P.O. Box 740241 Atlanta, GA 30374
Experian	1-888-397-3742	www.experian.com	P.O. Box 2104 Allen, TX 75013
TransUnion	1-800-680-7289	www.transunion.com	P.O. Box 6790 Fullerton, CA 92834

Contacting the Federal Trade Commission, Consumer Response Center, 1-877-438-4338, Room 130-B, 600 Pennsylvania Avenue, N.W. Washington, D.C., 20580, (http://www.ftc.gov/bcp/menus/consumer/data.shtm) which can provide additional advice regarding how to protect your personal information.

Notifying law enforcement or the office of your state Attorney General if you suspect that your personal information has been used fraudulently.

Although Experian's customer care team can answer most inquiries about this incident, for specific inquiries, please email Apria's Compliance/Legal group at Contact_Us@apria.com or contact us by mail at the following address: Apria Healthcare, Attention: HIPAA Privacy Officer, 26220 Enterprise Court, Lake Forest, CA 92630.

We sincerely apologize for this incident, regret any inconvenience it may cause you, and encourage you to take advantage of the Experian monitoring service.

Sincerely,

Doreen Bellucci
Vice President and Associate General Counsel

APRIA HEALTHCARE

26220 Enterprise Court
Lake Forest, California 92630
Tel 949.639.2000

August 15, 2012

Attorney General Michael Delaney
New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Security Incident

Dear Mr. Delaney:

Pursuant to New Hampshire Revised Statute sections 359-C:19, *et sec.*, we are writing to notify you of a security incident involving personal information of New Hampshire residents. On the evening of June 14, 2012, an unencrypted Apria Healthcare, Inc. ("Apria")-owned laptop was stolen from an Apria employee's locked vehicle in Phoenix, Arizona.

On June 15, 2012, the Apria employee notified law enforcement. We then began investigating the incident through our corporate compliance program. Apria's investigators and third-party digital forensics experts have determined that some of the files on the stolen laptop's hard drive contained certain personal information of certain New Hampshire residents. Typically these were patients who were referred to us by licensed healthcare practitioners for the purpose of serving their homecare needs; the data was provided as part of normal healthcare operations. Sorting through duplicative files that are believed to be on the laptop's hard drive and technical issues encountered by our digital forensics experts—technical issues that also make it harder for any thief to access the personal information—resulted in a longer time than initially expected to investigate the matter and provide this notice. At this time, we believe that approximately five (5) of residents in New Hampshire are affected. The personal information on the stolen laptop includes social security numbers, full names, and may have included date of birth and/or other personal or health information related to the individuals.

Although the laptop was not encrypted, it was password-protected. In addition to notifying law enforcement, we hired a private investigator to attempt to recover the laptop. Based on the circumstances under which the theft occurred, we believe this was a property crime and have no indication that any of the personal information has actually been accessed or misused.

Nevertheless, because protected health information and other confidential data were on the stolen laptop, we are providing all potentially affected individuals with notice of this data breach event in accordance with the federal requirements under the HIPAA breach notification rule at 45 CFR

§ 164.410 for HIPAA-covered entities. Further, we notified the Secretary of Health and Human Services and media outlets whose coverage area includes the potentially affected individuals' residences.

Notices are scheduled to be mailed to the five (5) New Hampshire residents potentially affected by this breach incident on August 16, 2012. Such notices are being sent by mail to each resident's record address on file with us.

We recognize the seriousness of this security incident and want to assure you that, in addition to our existing policies, procedures and employee training modules, we are taking additional precautions to minimize the chances of this type of incident happening again. We are retraining our employees on the importance of protecting the privacy and security of confidential information and are enhancing our internal safeguards to ensure the continued protection of all confidential and personal information in our care and custody. In particular, we are in the process of encrypting all of the company's laptops, a process that had begun long before this incident occurred but was delayed owing to some technical issues.

If you have any questions, I may be reached at 949-639-4141 to discuss this matter.

Very truly yours,

Ako S. Williams

Ako S. Williams
Assistant General Counsel

APRIA HEALTHCARE

26220 Enterprise Court
Lake Forest, CA 92630

September 28, 2012

Sample A. Sample
123 Anystreet
Anytown, US 12345-6789

Important: Health Information Security and Protection Notification

This is **official correspondence from Apria Healthcare, Inc.** (Apria) to inform you of a data security incident. On June 14, 2012, a laptop with password protection and owned by Apria was stolen from an employee's locked vehicle. Since that time, we have been investigating the incident thoroughly with the help of legal, computer, and compliance experts. Unfortunately, we learned that the files on the stolen laptop contained some of our current and past patients' personal information that was given to us as part of providing homecare equipment or service. We recently discovered that this may include your Social Security Number (SSN) and name, and may have included your date of birth and/or other personal or health information. We truly regret that this incident occurred and understand that it may concern you.

While we have no reason to believe that the information has been used by an inappropriate party, we have taken many steps to address the incident and are committed to fully protecting all of your personal information. To prevent this type of incident from happening again, we are retraining our employees, changing certain data storage policies and exploring new technologies to further protect company data.

To help you monitor the situation, Apria is providing free coverage by Experian's ProtectMyID™ Alert program for one year. This product helps detect possible misuse of your personal information and provides you with superior identity protection services. Once your ProtectMyID membership is activated, your credit report will be monitored daily for 50 leading indicators of identity theft. You'll receive periodic Credit Alerts from ProtectMyID on any key changes in your credit report.

In the unlikely case that identity theft is detected, ProtectMyID will assign a dedicated U.S.-based Identity Theft Resolution Agent who will walk you through the process of fraud resolution from start to finish.

Activate Your Free ProtectMyID Service now in Three Easy Steps:

1. **ENROLL** by November 30, 2012
2. **VISIT** the ProtectMyID Web Site: http://www.protectmyid.com/redeem or **CALL** 888-451-6562 to enroll
3. **PROVIDE** Your Personal Activation Code: 999999999

0346000000000000000101

63450002-004-000000025

For added protection, once you enroll, you will receive ExtendCARE™, which provides you with the same high level of Fraud Resolution support even after your ProtectMyID membership has expired after one year, at no additional cost to you.

Activate your membership today at http://www.protectmyid.com/redeem or call 888-451-6562 to register with the activation code found on page 1.

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 your credit report, or suspect that an item on it may be fraudulent, please contact Experian's customer care team at 888-451-6562.** Please note that you will be asked to provide your SSN in order to confirm your identity and enroll you in the program.

Other steps you may take include:

Checking your credit and similar accounts frequently over the next few years.

Notifying one of the three national credit reporting agencies to place a fraud alert, which will aid in preventing new credit accounts from being opened without your permission:

Credit Reporting Agency	Telephone Number	Website	Postal Address
Equifax	1-800-685-1111	www.equifax.com	P.O. Box 740241 Atlanta, GA 30374
Experian	1-888-397-3742	www.experian.com	P.O. Box 2104 Allen, TX 75013
TransUnion	1-800-680-7289	www.transunion.com	P.O. Box 6790 Fullerton, CA 92834

Contacting the Federal Trade Commission, Consumer Response Center, 1-877-438-4338, Room 130-B, 600 Pennsylvania Avenue, N.W. Washington, D.C., 20580, (http://www.ftc.gov/bcp/menus/consumer/data.shtm) which can provide additional advice regarding how to protect your personal information.

Notifying law enforcement or the office of your state Attorney General if you suspect that your personal information has been used fraudulently.

Although Experian's customer care team can answer most inquiries about this incident, for specific inquiries, please email Apria's Compliance/Legal group at Contact_Us@apria.com or contact us by mail at the following address: Apria Healthcare, Attention: HIPAA Privacy Officer, 26220 Enterprise Court, Lake Forest, CA 92630.

We sincerely apologize for this incident, regret any inconvenience it may cause you, and encourage you to take advantage of the Experian monitoring service.

Sincerely,

Doreen Bellucci
Vice President and Associate General Counsel