



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

Attorney General Michael Delaney
August 15, 2012
Page 2

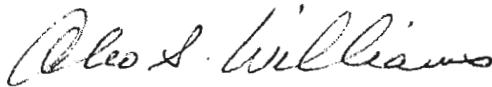
§ 164.410 for HIPAA-covered entities. Further, we notified the Secretary of Health and Human Services and media outlets whose coverage area includes the potentially affected individuals' residences.

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
Assistant General Counsel