



CONCORD REGIONAL April 18, 2008

VISITING NURSE

ASSOCIATION

Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Dear Sir or Madame:

We are notifying you of a security breach that resulted in the loss of personal information for fifteen clients of the Concord Regional Visiting Nurse Association. A CRVNA laptop computer was stolen from a staff member's vehicle on April 16, 2008. Personal data including the birth date and social security numbers for our clients was stored on the laptop. The risk of identity theft is low. The laptop security included three password levels to access the laptop data. The password levels include:

- a) A hard drive lock which requires a password to be entered prior to the boot up of the laptop.
- b) A password is then required to access the laptop Microsoft applications and the startup menu.
- c) And finally a third password is required to access the Horizon Home Care software which is the application that stored the personal information. In addition, the Horizon Home Care database folder has an encrypted system administrator password.

We have notified law enforcement regarding the theft. We are sending letters and will be calling or making visits to the clients whose data was stored on the laptop to alert them of the laptop theft. In addition, we will provide these clients with the information to help them place a fraud alert on their credit files with the three credit bureaus and we will assist them if necessary to make the calls.

If you have further questions or concerns, contact Violet M. Rounds at 603-224-4093 extension 4769.

Sincerely,

Violet M. Rounds
Chief Financial Officer/
Vice President of Administrative Services



April 18, 2008

CONCORD REGIONAL
VISITING NURSE
ASSOCIATION

Client Name and address

Dear Ms

We are contacting you because we have learned of a serious data security incident that involved some of your personal information. A CRVNA laptop computer was stolen from a staff member's vehicle on April 16, 2008. Your personal information was included in the files on the laptop. The risk of identity theft is low. It is unlikely that the person that stole the equipment will gain access to your information because of the three levels of security and encryption that was on the laptop. However, we feel it prudent to notify you of the concern.

We have notified law enforcement regarding the theft. We strongly encourage you to take preventative measures now to help prevent and detect any misuse of your information.

As a first step, we recommend you closely monitor your financial accounts and, if you see any unauthorized activity, promptly contact your financial institution. You also may want to consider requesting a free credit report. To order your free credit report, visit www.annualcreditreport.com or call toll free 1-877-322-8228.

To further protect yourself, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit report agencies at a number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Eperian
888-397-3742

Equifax
888-766-0008

TransUnion
800-680-7289

We apologize for any distress this situation may cause you. We are ready to assist you in any way.

If you have further questions or concerns, contact Violet M. Rounds at 603-224-4093 extension 4769.

Sincerely,

Violet M. Rounds
Chief Financial Officer/
Vice President of Administrative Services
Chief Privacy Officer